

CDP Private Cloud Data Services Release Notes

Date published: 2023-12-16

Date modified: 2024-10-18

The Cloudera logo is displayed in a bold, orange, sans-serif font. The word "CLOUDERA" is written in all caps, with the letter "E" stylized as a horizontal bar with a small triangle on its right side.

Legal Notice

© Cloudera Inc. 2024. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

What's new in CDP Private Cloud Data Services 1.5.4.....	4
Known issues for the CDP Private Cloud Data Services 1.5.4.....	4
Fixed Issues for the CDP Private Cloud Data Services 1.5.4.....	18
Repository Locations for 1.5.4.....	19
Fixed CVEs.....	19
Cumulative hotfixes.....	34
CDP Private Cloud Data Services 1.5.4-CHF1.....	34
Whats new in CDP Private Cloud Data Services1.5.4-CHF1.....	35
Known Issues in CDP Private Cloud Data Services 1.5.4-CHF1.....	35
Fixed Issues in CDP Private Cloud Data Services 1.5.4-CHF1.....	35
Repository Locations for 1.5.4-CHF1.....	36
Fixed Common Vulnerabilities and Exposures in 1.5.4 CHF1.....	36
CDP Private Cloud Data Services 1.5.4-CHF3.....	113
Whats new in CDP Private Cloud Data Services1.5.4-CHF3.....	114
Known Issues in CDP Private Cloud Data Services 1.5.4-CHF3.....	114
Repository Locations for 1.5.4-CHF3.....	116
Fixed Common Vulnerabilities and Exposures in 1.5.4 CHF3.....	117

What's new in CDP Private Cloud Data Services 1.5.4

New features in the 1.5.4 release of the CDP Private Cloud Management Console service.

CDP Private Cloud Data Services 1.5.4 support with 7.1.9 SP1.



Note: [Cloudera Manager 7.11.3 CHF7 Data Services](#) (version: 7.11.3.14) support CDP Private Cloud Data Services 1.5.4 release.



Note: Cloudera Manager 7.11.3 CHF8 does not support any CDP Private Cloud Data Services release.

Certifications

- Base (7.1.9 CHF 6, 7.1.7 SP3, 7.1.8 CHF22)
- CM 7.11.3 CHF 6 and CHF7
- Iceberg v2 GA on CDW, CDE, & CML with Ozone
- OEL (RHCK Kernel Only) 8.7, 8.8, 8.9, 9.1, 9.2, 9.3
- RHEL 8.7, 8.8, 8.9, 9.1, 9.2, 9.3
- K8s 1.27 and OCP 4.14

Stability and Resiliency: New prerequisite check in ECS Install Wizard

A new step is added in the ECS Install Wizard called Check Prerequisites. This ECS prerequisite checks fresh installations seamlessly and improves the overall installation experience for administrators. This step checks if the ECS hosts meet a list of minimum requirements before installation. For more information on this prerequisite check, see [Installing CDP Private Cloud Data Services using ECS](#).

DRS automatic backups

Starting from CDP Private Cloud Data Services 1.5.4, DRS automatic backups for Control Plane, Cloudera Data Warehouse (CDW), and Cloudera Data Engineering (CDE) are enabled by default on ECS clusters for new installations or after cluster upgrade to version 1.5.4 or higher. You can disable this option, if required. You can also configure the external storage in Longhorn for ECS, and then initiate DRS automatic backups to it.

Automatic backups (DRS) functionality is disabled by default on OCP clusters.

For more information, see [DRS automatic backups](#).

Authentication for Ingress TLS/SSL

A new property (`ssl_private_key_password`) is added to the Cloudera Manager to specify the password for the private key in the Ingress Controller TLS/SSL Server Certificate and Private Key file.

Improved Diagnostics

The `tez-site.xml` file is now included in the Management Console diagnostic bundle download.

Known issues for the CDP Private Cloud Data Services 1.5.4

This section lists known issues that you might run into while using the CDP Private Cloud Management Console service.

Known Issues in Management Console 1.5.4**OPSX-5147: OOM when retrieving size of Binary File**

Sometimes, diagnostics bundle collection fails to complete due to OOM issues.

Limit the time range for the diagnostics bundle.

OPSX-5148: Diagnostics Collection from UI w/ Default No Time Limit Should Not Invoke Timestamp Filtering

When the diagnostics collection is triggered through the UI, by default, "No Time Limit" is selected. Filtering of logs by timestamp is still observed.

No workaround available.

DOCS-20088/OPSX-4781: Vault pods may take long time to be ready during upgrades from 1.5.2 to 1.5.3

The 'vault-0' pod takes longer time to attach volume in some upgrade cases than usual. Due to the excess time taken the cluster upgrade may fail. But, usually in 15 minutes the volume can attach automatically and the pod would start running. In that case, the user can resume the upgrade.

No workaround available.

OPSX-5155: OS Upgrade | Pods are not starting after the OS upgrade from RHEL 8.6 to 8.8

After an OS upgrade and start of the ECS service, pods fail to come up due to stale state.

Restart the ECS cluster.

OPSX-5055: ECS upgrade failed at Unseal Vault step

During an ECS upgrade from 1.5.2 to 1.5.4 release, the vault pod fails to start due to an error caused by the Longhorn volume unable to attach to the host. The error is as below:

```
Warning FailedAttachVolume 3m16s (x166 over 5h26m) attachdetach-controller
AttachVolume.Attach failed for volume "pvc-0ba86385-9064-4ef9-9019-71976b4902a5" :
rpc error: code = Internal desc = volume pvc-0ba86385-9064-4ef9-9019-71976b4902a5
failed to attach to node host-1.cloudera.com with attachmentID
csi-7659ab0e6655d308d2316536269de47b4e66062539f135bf6012bfc8b41fc345: the volume is
currently attached to different node host-2.cloudera.com
```

Follow below steps provided by SUSE to ensure the Longhorn volume is correctly attached to the node where the vault pod is running.

```
# Find out the volume name that is failing to attach to the vault
pod.
For e.g. pvc-bc73e7d3-c7e7-468a-b8e0-afdb8033e40b from the pod
logs.
kubectl edit volumeattachments.longhorn.io -n longhorn-system
pvc-bc73e7d3-c7e7-468a-b8e0-afdb8033e40b

# Update the "spec:" section of the volumeattachment and replace
attachmentTickets section with {} as shown below and save.
spec:
  attachmentTickets: {}
  volume: pvc-bc73e7d3-c7e7-468a-b8e0-afdb8033e40b

# scale down the vault statefulset to 0 and scale it back up.
kubectl scale sts vault --replicas=0 -n vault-system
kubectl scale sts vault --replicas=1 -n vault-system
```

OPSX-4308: Display error in UI if listEnvironments failed

On the Environments page, if the `listEnvironments` API call fails, the error is hidden, and instead no environments are displayed, even though they do exist. This can be due to vault issues or connectivity issues.

No workaround available but the register environment page shows the error.

OPSX-4684: Start ECS command shows green(finished) even though start docker server failed on one of the hosts

The Docker service starts, but one or more Docker roles fail to start because the corresponding host is unhealthy.

Ensure the host is healthy. Start the the Docker role on the host.

OPSX-735: Kerberos service should handle Cloudera Manager downtime

The Cloudera Manager Server in the base cluster operates to generate Kerberos principals for Private Cloud. If there is downtime, you may observe Kerberos-related errors.

Resolve downtime on Cloudera Manager. If you encounter Kerberos errors, you can retry the operation (such as retrying creation of the Virtual Warehouse).

Known Issues in Management Console 1.5.3

OPSX-4754 [ECS Restart Stability] DaemonSet rollout process is stuck post rolling restart where DaemonSet kube-system/rke2-canal has not finished or progressed for at least 15 minutes

On RHEL 9.x, an ECS service DaemonSet rollout health alert appears in the Cloudera Manager after an ECS installation and a rolling restart.

To fix the DaemonSet rollout issue:

1. Edit the DaemonSet rke2-canal configuration file by running the following command:

```
KUBECTL -n kube-system edit ds/rke2-canal
```

Change the value of felixIptablesBackend from auto to Legacy and save the DaemonSet rke2-canal configuration file.

2. Reboot each node one-by-one.
3. Check to see if any of the nodes are cordoned off. If so, uncordon them:

```
[root@host-1 ~]# $KUBECTL get nodes
NAME STATUS ROLES AGE VERSION
host-1.ecs-restart1.kcloud.cloudera.com Ready,SchedulingDisabled control-plane,etcd,master 17h v1.26.10+rke2r1
host-2.ecs-restart1.kcloud.cloudera.com Ready <none> 17h v1.26.10+rke2r1
host-3.ecs-restart1.kcloud.cloudera.com Ready <none> 17h v1.26.10+rke2r1
host-4.ecs-restart1.kcloud.cloudera.com Ready <none> 17h v1.26.10+rke2r1
[root@host-1 ~]# $KUBECTL uncordon host-1.ecs-restart1.kcloud.cloudera.com
node/host-1.ecs-restart1.kcloud.cloudera.com uncordoned
[root@host-1 ~]# $KUBECTL get nodes
NAME STATUS ROLES AGE VERSION
host-1.ecs-restart1.kcloud.cloudera.com Ready control-plane,etcd,master 17h v1.26.10+rke2r1
host-2.ecs-restart1.kcloud.cloudera.com Ready <none> 17h v1.26.10+rke2r1
host-3.ecs-restart1.kcloud.cloudera.com Ready <none> 17h v1.26.10+rke2r1
host-4.ecs-restart1.kcloud.cloudera.com Ready <none> 17h v1.26.10+rke2r1
[root@host-1 ~]#
```

4. Ensure that the Vault is unsealed. , To unseal the vault in Cloudera Manager navigate to Clusters ECS <***ECS SERVICES***> such as ECS-1 or ECS-2 Actions Unseal Vault .
5. Wait for five to six minutes.
6. Check for longhorn pods that fail to come up on any of the hosts:

```
[root@host-1 ~]# kubectl -o wide get pods -n longhorn-system |
grep -v "Running" | grep -v "Completed"
```

NAMESPACE	NAME	READY
STATUS	RESTARTS	AGE
NODE		IP
NOMINATED NODE	READINESS GATES	
longhorn-system		longhorn-csi-plugin-
frwnw		2/3
CrashLoopBackOff	14 (3m51s ago)	6h20m 10.x.x.x
host-1.upgr-ecs-ext.kcloud.cloudera.com		<none>
<none>		
longhorn-system		longhorn-manager-lgzm
b		0/1
CrashLoopBackOff	7 (97s ago)	6h24m 10.x.x.x
host-1.upgr-ecs-ext.kcloud.cloudera.com		<none>
<none>		

7. Reboot the host (In this case the host is: *host-1.upgr-ecs-ext.kcloud.cloudera.com*).
8. Wait for 15-30 minutes for pods to come up.
9. Post ECS reboot, if you notice buildkit pods in the following CrashLoopBackOff state, then delete those buildkit pods:

```
[root@host-1 ~]# kubectl -o wide get pods | grep -v "Running"
| grep -v "Completed"
```

NAMESPACE	NAME	READY	STATUS
	RESTARTS	AGE	IP
			NOMINATED NODE
			READINESS
GATES			
quasar-sk12-host-1			buildkit-2jdmw
		2/3	CrashLoopBackOff
	14 (3m51s ago)	6h20m	10.x.x.x
ext.kcloud.cloudera.com		<none>	host-1.upgr-ecs-
			<none>
quasar-sk12-host-1			buildkit-k20smc
		0/1	CrashLoopBa
ckOff	7 (97s ago)	6h24m	10.x.x.x
gr-ecs-ext.kcloud.cloudera.com		<none>	host-2.up
			<none>

You can delete the above buildkit pods by one of the following ways:

- On the Cloudera Manager UI, navigate to Clusters ECS <***ECS SERVICES***> such as ECS-1 or ECS-2 Web UI ECS Web UI Delete .
- Run the following command to delete all such buildkit pods:

```
[root@host-1 ~]# kubectl delete pod buildkit-2jdmw -n quasar
-sk12-host-1
```

Wait for the buildkit pods to start back up.

OPSAPS-69892: kube-proxy failure causing issues with cluster

After rebooting/restarting an ECS agent node, the kube-proxy Linux process may not start due to a race condition in the kubelet. When this happens, ECS cluster networking and other services – such as Vault, DNS, authentication, Longhorn storage, etc. – are affected. At the Kubernetes pod level, errors such as "connection refused", "connection timed out" and "i/o timeout" may be observed. If

you suspect possible networking issues in your ECS cluster, checking kube-proxy is a good first step.

To fix this issue, perform the following steps on all of the affected nodes:

1. To identify which agent needs to be restarted, check the status of each kube-proxy pod to make sure it is in the "ready" state by running the following command on each host in the cluster.

```
kubectl describe pod [***POD-NAME***] -n kube-system
```

Here, [***POD-NAME***] should have a format such as: kube-proxy-<hostname>.

In the Conditions section of the describe pod output, confirm that the "ready" condition is "True".

```
Conditions:
  Type              Status
  Initialized        True
  Ready              True
  ContainersReady    True
  PodScheduled       True
```

Another option is to run the following command:

```
kubectl get pods -n kube-system -l component=kube-proxy -o go-template='{{range .items}}
{{.metadata.name}}{{"\n"}}{{"  "}}{{range .status.conditions}}
{{ if eq .type "Ready" }}
Ready:{{.status}}{{"\n\n"}}{{end}}{{end}}{{end}}'
```

The sample output displays the status of all of the kube-proxy pods in the cluster:

```
kube-proxy-host-1.cloudera.com
Ready:True

kube-proxy-host-2.cloudera.com
Ready:True

kube-proxy-host-3.cloudera.com
Ready:True
```

2. If the "ready" state is False, kube-proxy is not functioning properly, regardless of whether the kube-proxy process is running on that host or not. On each of the affected nodes, run the following command to delete the kube-proxy pod manifest:

```
rm /var/lib/rancher/rke2/agent/pod-manifests/kube-proxy.yaml
```

3. Start the agent role.

After the agent role is started, you may not immediately see the kube-proxy process running, but a new kube-proxy process should start shortly. Check the pod status to make sure it is ready. After all of the problem agents have been restarted, the cluster may complain that the vault is sealed – if so, unseal it. At this point, the Control Plane should be functioning properly.

Additional details about this issue are available here: <https://www.suse.com/support/kb/doc/?id=000021284>

OPSX-4766: [ECS Restart]| Host Reboot | start command failed with error - "Timed out waiting for kube-apiserver to be ready"

In an ECS cluster with HA enabled, ECS Start fails with an error after stopping the cluster and rebooting the hosts.

Steps to reproduce:

1. Stop ECS.
2. Reboot hosts.
3. Start ECS.

The start command fails with the following error message:

"Timed out waiting for kube-apiserver to be ready"

Option 1:

Start each master role instance individually without waiting each node to be up and running.

Option 2:

If Option 1 does not work, follow the steps from SUSE to recover the cluster: https://docs.rke2.io/backup_restore#cluster-reset

Known Issues in Management Console 1.5.2

OPSAPS-68923: CM - After CM upgrade from 7.9.5 to 7.11.3.x ECS cluster showing stale config

After Cloudera Manager upgrade from 7.9.5 to 7.11.3.x, an ECS 1.5.0 cluster may show a stale config to add `""limit_fds": 1048576"`

This can be ignored – no restart of the ECS cluster is necessary. When the ECS 1.5.0 cluster is upgraded to 1.5.2, the stale config will be resolved.

OPSX-4594: [ECS Restart Stability] Post rolling restart few volumes are in detached state (vault being one of them)

After rolling restart there may be some volumes in detached state.

1. Open the Longhorn UI to view the detached volumes.
2. Perform the following operations for each volume in a detached state:
 - a. Identify the workload name and type from the volume details.
 - b. Identify the workload and number of replicas using kubectl or the Kubernetes UI.
 - c. Scale the workload down to 0.
 - d. Wait for the pods associated with the workload to fully terminate.
 - e. Scale up the workload up to the number of replicas it had originally.

To prevent this issue, use the Longhorn UI to set the number of replicas for the volume to at least 3.

OPSAPS-68558: [7.9.5->7.11.3.2] CM upgrade failed with BeanCreationException: Error creating bean with name 'com.cloudera.server.cmf.TrialState'

After upgrading the Cloudera Manager package, the Cloudera Manager Server does not start. An error about "Active Commands" is shown in the Cloudera Manager Server log.

This may happen when the Private Cloud Data Services Control Plane is actively issuing requests to Cloudera Manager while an upgrade is being performed.

Before upgrading Cloudera Manager make sure there are no active commands. If there are any active commands, wait for them to complete before starting a Cloudera Manager upgrade.

If Cloudera Manager restart fails after upgrade due to an active `getClientConfig` command, check the Cloudera Manager server log for a "There are 1 active commands of type GetClientConfigFiles" error. This may block a Cloudera Manager restart after upgrade. Use the following steps to resolve this issue:

1. Login to Cloudera Manager database.

2. Search for any active GetClientConfigFiles command in the COMMANDS table.

```
UPDATE COMMANDS SET active=0,success=false,state='CANCELLED'
where command_id=<command_id>;
```

3. Delete these entries, including foreign key dependencies, in the following tables:

- PROCESSES
- PROCESSES_DETAIL
- COMMANDS_DETAIL

```
cm=> DELETE FROM COMMANDS where command_id=1546340765;
ERROR: update or delete on table "commands" violates foreign
key constraint "fk_process_command" on table "processes"
DETAIL: Key (command_id)=(1546340765) is still referenced from
table "processes".
cm=>
cm=> DELETE FROM processes where command_id=1546340765;
ERROR: update or delete on table "processes" violates foreign
key constraint "fk_processes_detail_process" on table "processes_detail"
DETAIL: Key (process_id)=(1546340766) is still referenced from
table "processes_detail".
cm=>
cm=> ^
cm=> DELETE FROM processes_detail where process_id=1546340766;
DELETE 1
cm=> DELETE FROM processes where command_id=1546340765;
DELETE 1
cm=> DELETE FROM COMMANDS where command_id=1546340765;
ERROR: update or delete on table "commands" violates foreign
key constraint "fk_commands_detail_command" on table "commands_detail"
DETAIL: Key (command_id)=(1546340765) is still referenced from
table "commands_detail".
cm=>
cm=> DELETE FROM commands_detail where command_id=1546340765;
DELETE 1
cm=> DELETE FROM COMMANDS where command_id=1546340765;
DELETE 1
```

4. Restart the Cloudera Manager server.

OPSX-4392: Getting the real client IP address in the application

CML has a feature for adding the audit event for each user action ([Monitoring User Events](#)). In Private Cloud, instead of the client IP, we are getting the internal IP, which is logged into the internal DB.

In ECS, add the [enable-real-ip](#) configuration as true for the nginx ingress controller:

```
apiVersion: v1
data:
  allow-snippet-annotations: "true"
  enable-real-ip: "true" <<<<<<<<<<<< new config
kind: ConfigMap
metadata:
  annotations:
    meta.helm.sh/release-name: rke2-ingress-nginx
    meta.helm.sh/release-namespace: kube-system
  creationTimestamp: "2023-05-09T04:54:53Z"
  labels:
    app.kubernetes.io/component: controller
    app.kubernetes.io/instance: rke2-ingress-nginx
```

```
app.kubernetes.io/managed-by: Helm
app.kubernetes.io/name: rke2-ingress-nginx
app.kubernetes.io/part-of: rke2-ingress-nginx
app.kubernetes.io/version: 1.6.4
helm.sh/chart: rke2-ingress-nginx-4.5.201
name: rke2-ingress-nginx-controller
namespace: kube-system
resourceVersion: "162559439"
uid: cca67b0c-bc05-4e1f-8439-7d44323f4624
```

In OCP, you may be able to configure this using [HAproxy with X-forward-for pass to OpenShift 4](#).

OPSX-4552: [ECS Restart] One of the docker servers failed to come up after starting the cluster post hosts reboot

At times the Docker server may fail to come up and return the following error message:

```
/var/run/docker.sock: Is a directory
```

On the Docker server role host, remove the /var/run/docker.sock directory, then restart the Docker server role.

CDPVC-1137, CDPAM-4388, COMPX-15083, and COMPX-15418: OpenShift Container Platform version upgrade from 4.10 to 4.11 fails due to a Pod Disruption Budget (PDB) issue

PDB can prevent a node from draining which makes the nodes to report the “Ready,SchedulingDisabled” state. As a result, the node is not updated to correct the Kubernetes version when you upgrade OCP from 4.10 to 4.11.

To resolve this issue, confirm that the upgrade has failed due to the PDB issue, and then manually delete the PDBs from the Private Cloud namespace.

1. Run the following command to check whether the nodes are stuck in the “Ready,SchedulingDisabled” state:

```
oc get nodes
```

2. Get the machine config daemon details of the particular pod as follows:

```
oc get po -n openshift-machine-config-operator -l 'k8s-app=machine-config-daemon' -o wide
```

3. Check the logs of the machine config operator of that particular node as follows:

```
oc logs -f -n openshift-machine-config-operator [***MACHINE-CONFIG-DAEMON-NAME***] -c machine-config-daemon
```

Replace [***MACHINE-CONFIG-DAEMON-NAME***] with the actual machine config daemon name.

You may see one of the following errors in the node logs:

- error when evicting pods/cdp-release-cpx-liftie-****" -n "[***PRIVATE-CLOUD-NAMESPACE***] Cannot evict pod as it would violate the pod's disruption budget
- error when evicting pods/"cdp-release-cluster-proxy-[*****]" -n "[***PRIVATE-CLOUD-NAMESPACE***] Cannot evict pod as it would violate the pod's disruption budget

Delete the PDB from the Private Cloud namespace as follows:

- a. Obtain the PDB for the cdp-release-cluster-proxy namespace:

```
oc get pdb -n [***PRIVATE-CLOUD-NAMESPACE***] | grep cdp-release-cluster-proxy
```

- b. Back up the PDB:

```
oc get pdb [***PDB-NAME-OF-CLUSTER-PROXY***] -n [***PRIVATE-CLOUD-NAMESPACE***] -o yaml >> [***BACKUP-FILE-NAME***].yaml
```

- c. Delete the PDB:

```
oc delete pdb [***PDB-NAME-OF-CLUSTER-PROXY***] -n [***PRIVATE-CLOUD-NAMESPACE***]
```

Repeat the steps to delete the cdp-release-cpx-liftie PDB as well.

PULSE-944 and PULSE-941 Observability namespace not created after platform upgrade from 151 to 152

The Cloudera Observability namespace is not created after a platform upgrade from PvC DS 1.5.1 to PvC DS 1.5.2.

During the creation of the resource pool the Cloudera Observability namespace is provided by the CDP Private Cloud Service. If the provisioning flow is not completed, such as due to a timing difference between the start of the computeAPI pod and the call to the computeAPI pod by the service, the namespace is not created.

Trigger the Cloudera Observability namespace deployment by restarting the pvcservice pod.

PULSE-921 Observability namespace has no pods

The Cloudera Observability namespace should have the same number of pods and nodes. When the Cloudera Observability namespace has no pods the prometheus-node-exporter-1.6.0 helm release state becomes invalid and the CDP Private Cloud Service is unable to uninstall and reinstall the namespace. Also, as the Node Exporter is not installed into the Cloudera Observability namespace its metrics are unavailable when querying Prometheus in the control plane, for example the node_cpu_seconds_total metric.

Manually uninstall the invalid helm release with the --debug flag, verify that there are no helm releases listed by running `-n observability -a`, and then trigger the deployment process by restarting the pvcservice pod in the control plane.

PULSE-697 Add node-exporter to PvC DS

When expanding a cluster with new nodes and there is insufficient CPU and memory resources, the Node Exporter will encounter difficulties deploying new pods on the additional nodes.

To ensure sufficient resource allocation, such as when the Cloudera Observability namespace requires adjustment, delete the existing namespace and restart the pvcservice pod. This automatically initiates the creation of the Cloudera Observability namespace with the appropriate resource allocation.



Note: During the namespace recreation process the Node Exporter metrics are temporarily unavailable.

PULSE-935 Longhorn volumes are over 90% of the capacity alerts on Prometheus volumes

Cloudera Manager displays the following alert about your Prometheus volumes: Concerning: Firing alerts for Longhorn: The actual used space of Longhorn volume is over 90% of the capacity.

Longhorn stores historical data as snapshots that are calculated with the active data for the volume's actual size. This size is therefore greater than the volume's nominal data value.

When the alert is displayed on the Cloudera Manager UI and it is related to Longhorn volumes used by Prometheus, ignore. For more information, see the Longhorn space consumption guidelines in the Longhorn documentation.

PULSE-937 Private-Key field change in Update Remote Write request does not reflect in enabling the metric flow

When using the Management Console UI for Remote Storage the Disable option does not deactivate the remote write configuration, even when the action returns a positive result message. Therefore, when disabling a remote storage configuration use the CLI client to disable the remote storage configuration directly from the API.

At this time when a remote storage configuration is incorrect, do not use the Edit or Disable option from the configuration's Actions menu (ellipsis icon) to change its configuration. Instead, delete the remote storage's configuration from the configuration's Actions menu with the Remove Configuration action and then re-create the remote write configuration with the Delete and Create operations of the API, using the CLI client.

PULSE-841 Disabling the remote write configuration logs an error in both cp prometheus and env prometheus

When a metric replication is set up between the cluster and Cloudera Observability and the connection is disabled or deleted, Prometheus writes an error message that states that it cannot replicate the metrics.

No workaround is required. After a few minutes the errors are no longer logged and Prometheus no longer tries to replicate the metrics.

PULSE-895 Disabling the remote write config in the UI is broken in cdp-pvc

The Remote Write Enable and Disable options in the Management Console's User Interface do not work when a Remote Storage configuration is created with a requestSignerAuth type from either the HTTP API or using the CDP-CLI tool.

At this time, do not use the Enable or Disable options from the Remote Storage configuration's Actions menu in the Management Console's UI. Instead, enable or disable the configuration from the HTTP API or using the CDP-CLI tool.

PULSE-936 No Alert to prompt the metric flow being affected b/c of wrong private key configuration

A remote write alert was not triggered when the wrong private key was used in a Remote Storage configuration.

No workaround. Incorrect configuration settings, such as in this case where a bad private key was used, may block the forwarding of metrics. When creating a Remote Storage configuration you must carefully verify each configuration setting.

Known Issues in Management Console 1.5.1

External metadata databases are no longer supported on OCP

As of CDP Private Cloud Data Services 1.5.1, external Control Plane metadata databases are no longer supported. New installs require the use of an embedded Control Plane database. Upgrades from CDP Private Cloud Data Services 1.4.1 or 1.5.0 to 1.5.1 are supported, but there is currently no migration path from a previous external Control Plane database to the embedded Control Plane database. Upgrades from 1.4.0 or 1.5.0 with external Control Plane metadata databases also require additional steps, which are described in the CDP Private Cloud Data Services 1.5.1 upgrade topics.

DOCS-15855: Networking API is deprecated after upgrade to CDP Private Cloud Data Services 1.5.1 (K8s 1.24)

When the control plane is upgraded from 1.4.1 to 1.5.1, the Kubernetes version changes to 1.24. The Livy pods running in existing Virtual Clusters (VCs) use a deprecated networking API for creating ingress for Spark driver pods. Because the old networking API is deprecated and does not exist in Kubernetes 1.24, any new job run will not work for the existing VCs.

CDPQE-24295: Update docker client on docker.lab.eng.hortonworks machine

When you attempt to execute the Docker command to fetch the Cloudera-provided images into your air-gapped environment, you may encounter an issue where Docker pulls an incorrect version of the HAProxy image, especially if you are using an outdated Docker client. This situation arises due to the Cloudera registry containing images with multiple platform versions. Unfortunately, older Docker clients may lack the capability to retrieve the appropriate architecture version, such as amd64.

Update the Docker client. It has been demonstrated that Docker 20.10.5 and later versions have been successful in resolving this problem.

OPSX-4266: ECS upgrade from 1.5.0 to 1.5.1 is failing in Cadence schema update job

When upgrading from ECS 1.5.0 to 1.5.1, the CONTROL_PLANE_CANARY fails with the following error:

```
Firing alerts for Control Plane: Job did not complete in time, Job failed to complete.
```

And the cdp-release-cdp-cadence-schema-update job fails.

Use the following steps to manually execute the job:

1. Export the job manifest into a file:

```
kubectl get job cdp-release-cdp-cadence-schema-update -n <cdp>
-o yaml > job.yaml
```

2. Delete the cdp-release-cdp-cadence-schema-update job:

```
kubectl delete job cdp-release-cdp-cadence-schema-update -n
<cdp>
```

3. Remove runtime information from the manifest, such as:

```
resourceVersion
uid
selector
  matchLabels
    controller-uid
labels
  controller-uid
status section
```

4. Create the job:

```
kubectl apply -f job.yaml
```

OPSX-4076:

When you delete an environment after the backup event, the restore operation for the backup does not bring up the environment.

Create the environment manually.

OPSX-4024: CM truststore import into unified truststore should handle duplicate CommonNames

If multiple CA certificates with the exact same value for the Common Name field are present in the Cloudera Manager truststore when a Private Cloud Data Services cluster is installed, only one of them may be imported into the Data Services truststore. This may cause certificate errors if an incorrect/old certificate is imported.

Remove old certificates from the Cloudera Manager truststore, and ensure certificates have unique Common Names.

COMOPS-2822: OCP error x509: certificate signed by unknown authority

The error x509: certificate signed by unknown authority usually means that the Docker daemon that is used by Kubernetes on the managed cluster does not trust the self-signed certificate.

Usually the fix is to copy the certificate to the path below on all of the worker nodes in the cluster:

```
/etc/docker/certs.d/<your_registry_host_name>:<your_registry_host_port>/ca.crt
```

OPSX-3073 [ECS] First run command failed at setup storage step with error "Timed out waiting for local path storage to come up"

Pod stuck in pending state on host for a long time. Error in Role log related to CNI plugin:

Events:

Type	Reason	Age	From
Warning	FailedCreatePodSandBox	3m5s (x269 over 61m)	kubelet
(combined from similar events):			
Failed to create pod sandbox: rpc error: code = Unknown desc = failed to setup network for sandbox "70427e9b26fb014750dfe4441fdfae96cb4d73e3256ff5673217602d503e806f": failed to find plugin "calico" in path [/opt/cni/bin]			

Delete the cni directory on the host failing to launch pods:

```
ssh root@ecs-hal-p-7.vpc.cloudera.com rm -rf /var/lib/cni
```

Restart the canal pod running on that host:

```
kubectl get pods -n kube-system -o wide | grep ecs-hal-p-7.vpc.cloudera.com
kube-proxy-ecs-hal-p-7.vpc.cloudera.com 1/1
Running 0 11h 10.65.52.51 ecs-hal-p-7.vpc.cloudera.com <none> <none>
rke2-canal-1lkc9 2/2
Running 0 11h 10.65.52.51 ecs-hal-p-7.vpc.cloudera.com <none> <none>
rke2-ingress-nginx-controller-dqtz8 1/1 R
unning 0 11h 10.65.52.51 ecs-hal-p-7.vpc.cloudera.com <none> <none>
kubectl delete pod rke2-canal-1lkc9 -n kube-system
```

OPSX-3528: [Pulse] Prometheus config reload fails if multiple remote storage configurations exist with the same name

It is possible to create multiple remote storage configurations with the same name. However, if such a situation occurs, the metrics will not flow to the remote storage as the config reload of the original prometheus will fail.

At any point in time, there should never be multiple remote storage configurations existing that have the same name.

OPSX-1405: Able to create multiple CDP PVC Environments with the same name

If two users try to create an environment with the same name at the same time, it might result in an unusable environment.

Delete the environment and try again with only one user trying to create the environment.

OPSX-1412: Creating a new environment through the CDP CLI reports intermittently that "Environment name is not unique" even though it is unique

When multiple users try to create the same environment at the same time or use automation to create an environment with retries, create environment may fail on collision with a previous request to create an environment.

Delete the existing environment, wait 5 minutes, and try again.

Known Issues in Management Console 1.5.0**Somehow the Rebuilding field inside volume.meta is set to true causing the volume to get stuck in attaching/detaching loop**

This is a condition that can occur in ECS Longhorn storage.

Since the volume has only 1 replica in this case, we can:

1. Scale down the workload. The Longhorn volume will be detached.
2. Wait for the Longhorn volume to be detached.
3. SSH into the node that has the replica.
4. cd into the replica folder (for example, `/longhorn/replicas/pvc-126d40e2-7bff-4679-a310-e444e84df267-1a5dc941`).
5. Change the "Rebuilding" field from true to false in the volume.meta file.
6. Scale up the workload to attach the volume.

Known Issues in Management Console identified before 1.5.0**INSIGHT-2469: COE Insight from case 922848: Not able to connect to bit bucket**

After installing CML on an ECS cluster, users were not able to connect the internal bitbucket repo.

Workaround:

In this case the MTU of the ECS virtual network interfaces were larger than that of host external interface, which may cause the network requests from ECS containers to get truncated.

The Container Network Interface (CNI) is a framework for dynamically configuring networking resources. CNI integrates smoothly with Kubernetes to enable the use of an overlay or underlay network to automatically configure the network between pods. Cloudera ECS uses Calico as the CNI network provider.

The MTU of the pods' virtual network interface can be seen by running the `ifconfig` command.

The default MTU of the virtual network interfaces is 1450.

The MTU setting of the virtual interfaces is stored as a configmap in the kube-system namespace. To modify the MTU, edit the rke2-canal-config configmap.

```
$ /var/lib/rancher/rke2/bin/kubectl --kubeconfig  
/etc/rancher/rke2/rke2.yaml --namespace kube-system  
edit cm rke2-canal-config
```

Find the veth_mtu parameter in the YAML content. Modify the default value of 1450 to the required MTU size.

Next, restart the rke2-canal pods from the kube-system namespace. There will be rke2-canal pods for each ECS node.

After the pods are restarted, all subsequent new pods will use the new MTU setting. However, existing pods that are already running will remain on the old MTU setting. Restart all of the pods to apply the new MTU setting.

OPSX-2484: FileAlreadyExistsException during timestamp filtering

The timestamp filtering may result in FileAlreadyExistsException when there is a file with same name already existing in the tmp directory.

None

OPSX-2772: For Account Administrator user, update roles functionality should be disabled

An Account Administrator user holds the biggest set of privileges, and is not allowed to modify via current UI, even user try to modify permissions system doesn't support changing for account administrator.

CDP Private Cloud Data Services ECS Installation: Failed to perform First Run of services.

If an issue is encountered during the Install Control Plane step of Containerized Cluster First Run, installation will be re-attempted infinitely rather than the command failing.

Since the control plane is installed and uninstalled in a continuous cycle, it is often possible to address the cause of the failure while the command is still running, at which point the next attempted installation should succeed. If this is not successful, abort the First Run command, delete the Containerized Cluster, address the cause of the failure, and retry from the beginning of the Add Cluster wizard. Any nodes that are re-used must be cleaned before re-attempting installation.

Environment creation through the CDP CLI fails when the base cluster includes Ozone

Problem: Attempt to create an environment using the CDP command-line interface fails in a CDP Private Cloud Data Services deployment when the Private Cloud Base cluster is in a degraded state and includes Ozone service.

Workaround: Stopping the Ozone service temporarily in the Private Cloud Base cluster during environment creation prevents the control plane from using Ozone as a logging destination, and avoids this issue.

Filtering the diagnostic data by time range might result in a FileAlreadyExistsException

Problem: Filtering the collected diagnostic data might result in a FileAlreadyExistsException if the /tmp directory already contains a file by that name.

There is currently no workaround for this issue.

Kerberos service does not always handle Cloudera Manager downtime

Problem: The Cloudera Manager Server in the base cluster must be running to generate Kerberos principals for CDP Private Cloud. If there is downtime, you might observe Kerberos-related errors.

Resolve downtime issues on Cloudera Manager. If you encounter Kerberos errors, you can retry the concerned operation such as creating Virtual Warehouses.

Updating user roles for the admin user does not update privileges

In the Management Console, changing roles on the User Management page does not change privileges of the admin user.

None

Upgrade applies values that cannot be patched

If the size of a persistent volume claim in a Containerized Cluster is manually modified, subsequent upgrades of the cluster will fail.

None

Fixed Issues for the CDP Private Cloud Data Services 1.5.4

This section lists the issues that have been fixed since the last release of the CDP Private Cloud Management Console service.

Fixed Issues in Management Console 1.5.4

TSB 2024-746: Concurrent compactions from Spark and modify statements from Hive and Impala can corrupt Iceberg tables.

This issue has been fixed.

TSB 2024-745: Impala returns incorrect results for Iceberg V2 tables when optimized operator is being used in CDW.

This issue has been fixed.

TSB 2024-758: Truncate command on Iceberg V2 branches cause unintentional data deletion.

This issue has been fixed.

OPsx-4446: Duplicate entries in cdp-pvc-truststore

Duplicate certificates are no longer available in the unified truststore.

OPsx-4650: CM - OCP pvc install Wizard - fails if route name is too long

The kubernetes namespace field is limited to 30 characters. This does not affect existing installations.

OPsx-3666: mlx_crud_app DB connection fails with error "unable to create connection: x509: certificate relies on legacy Common Name field, use SANs instead"

If you are upgrading from CDP Private Cloud Data Services 1.4.1 or 1.5.0 to 1.5.1 or higher versions, and you were previously using an external database, you must regenerate the DB certificate with SAN before upgrading to CDP Private Cloud Data Services 1.5.1 or higher versions.

OPsx-4225: Upgrade failed as cadence pods are crashlooping post upgrade

When doing a fresh install of CDP Private Cloud Data Services 1.5.1, external metadata databases are no longer supported. Instead, the CDP Private Cloud Data Services installer will create an embedded database pod by default, which runs inside the Kubernetes cluster to host the databases required for installation.

If you are upgrading from CDP Private Cloud Data Services 1.4.1 or 1.5.0 to 1.5.1 or higher versions, and you were previously using an external database, you must run the following psql commands to create the required databases. You should also ensure that the two new databases are owned by the common database users known by the control plane.

```
CREATE DATABASE db-cadence;
CREATE DATABASE db-cadence-visibility;
```

DOCS-19913: OCP upgrade – OCP namespace name must be 29 characters or less

The kubernetes namespace field is limited to 30 characters in OCP. This does not affect existing installations.

COMPX-15475: [CM ECS UPG][150-152] post upgrade prometheus-node-exporter-1.6.0 pod stuck in pending state

Applications, and their pods, that were running before an upgrade are no longer rejected. They get moved to a temporary queue during initialisation if they cannot be placed in the requested queue. This prevents a secondary issue, node rejections, from occurring which caused the pending pods.

OPSAPS-66166: FreeIPA cadminrole needs more privileges for PvC+ after upgrade

After upgrade, the Cloudera Manager admin role may be missing the Host Administrators privilege in an upgraded cluster.

The cluster administrator should run the following command to manually add this privilege to the role.

```
ipa role-add-privilege <cadminrole> --privileges="Host Administ  
rators"
```

For more information, see [Upgrade from 1.5.2 or 1.5.3 to 1.5.4 \(ECS\)](#).

Repository Locations for 1.5.4

The URLs for CDP Private Cloud Data Services 1.5.4-CHF1 are listed in the following table:

URL Type	Repository Location
Index	<code>https://username:password@archive.cloudera.com/p/cdp-pvc-ds/1.5.4/</code>
Manifest	Repository: <code>https://username:password@archive.cloudera.com/p/cdp-pvc-ds/1.5.4/manifest.json</code>
Parcels	Repository: <code>https://username:password@archive.cloudera.com/p/cdp-pvc-ds/1.5.4/parcels/</code>

List of fixed Common Vulnerabilities and Exposures in 1.5.4

Review the Common vulnerabilities and Exposures (CVEs) that were fixed in this release of CDP Private Cloud Data Services.

- [CVE-2023-27539](#): A denial of service vulnerability was found in rubygem-rack in how it parses headers. A carefully crafted input can cause header parsing to take an unexpected amount of time, possibly resulting in a denial of service.
- [DSA-5692-1](#): ghostscript - security update
- [CVE-2024-33871](#): An issue was discovered in Artifex Ghostscript before 10.03.1. contrib/opvp/gdevopvp.c allows arbitrary code execution via a custom Driver library, exploitable via a crafted PostScript document. This

occurs because the Driver parameter for opvp (and oprp) devices can have an arbitrary name for a dynamic library; this library is then loaded.

- [CVE-2024-33870](#): An issue was discovered in Artifex Ghostscript before 10.03.1. There is path traversal (via a crafted PostScript document) to arbitrary files if the current directory is in the permitted paths. For example, there can be a transformation of `../../foo` to `./../../foo` and this will grant access if `./` is permitted.
- [CVE-2024-33869](#): An issue was discovered in Artifex Ghostscript before 10.03.1. Path traversal and command execution can occur (via a crafted PostScript document) because of path reduction in `base/gpmisc.c`. For example, restrictions on use of `%pipe%` can be bypassed via the `aa/../../%pipe%command# output filename`.
- [CVE-2024-29510](#): Artifex Ghostscript before 10.03.1 allows memory corruption, and SAFER sandbox bypass, via format string injection with a `uniprint` device.
- [DSA-5679-1](#): `less` - security update
- [DSA-5682-2](#): `glib2.0` - regression update
- [DSA-5682-1](#): `glib2.0` - security update
- [CVE-2024-23653](#): BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. In addition to running containers as build steps, BuildKit also provides APIs for running interactive containers based on built images. It was possible to use these APIs to ask BuildKit to run a container with elevated privileges. Normally, running such containers is only allowed if special ``security.insecure`` entitlement is enabled both by buildkitd configuration and allowed by the user initializing the build request. The issue has been fixed in v0.12.5. Avoid using BuildKit frontends from untrusted sources.
- [CVE-2024-23652](#): BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. A malicious BuildKit frontend or Dockerfile using `RUN --mount` could trick the feature that removes empty files created for the mountpoints into removing a file outside the container, from the host system. The issue has been fixed in v0.12.5. Workarounds include avoiding using BuildKit frontends from an untrusted source or building an untrusted Dockerfile containing `RUN --mount` feature.
- [CVE-2023-36665](#): `protobuf.js` (aka `protobufjs`) 6.10.0 through 7.x before 7.2.5 allows Prototype Pollution, a different vulnerability than [CVE-2022-25878](#). A user-controlled protobuf message can be used by an attacker to pollute the prototype of `Object.prototype` by adding and overwriting its data and functions. Exploitation can involve: (1) using the function `parse` to parse protobuf messages on the fly, (2) loading `.proto` files by using `load/loadSync` functions, or (3) providing untrusted input to the functions `ReflectionObject.setParsedOption` and `util.setProperty`.
- [CVE-2024-22682](#): `DuckDB` $\leq 0.9.2$ and `DuckDB extension-template` $\leq 0.9.2$ are vulnerable to malicious extension injection via the custom extension feature.
- [CVE-2022-30123](#): A sequence injection vulnerability exists in `Rack` $< 2.0.9.1$, $< 2.1.4.1$ and $< 2.2.3.1$ which could allow is a possible shell escape in the `Lint` and `CommonLogger` components of `Rack`.
- [CVE-2023-38545](#): This flaw makes `curl` overflow a heap based buffer in the `SOCKS5` proxy handshake. When `curl` is asked to pass along the hostname to the `SOCKS5` proxy to allow that to resolve the address instead of it getting done by `curl` itself, the maximum length that hostname can be is 255 bytes. If the hostname is detected to be longer than 255 bytes, `curl` switches to local name resolving and instead passes on the resolved address only to the proxy. Due to a bug, the local variable that means 'let the host resolve the name' could get the wrong value during a slow `SOCKS5` handshake, and contrary to the intention, copy the too long hostname to the target buffer instead of copying just the resolved address there.
- [CVE-2023-32002](#): The use of ``Module._load()`` can bypass the policy mechanism and require modules outside of the `policy.json` definition for a given module. This vulnerability affects all users using the experimental policy mechanism in all active release lines: 16.x, 18.x and, 20.x. Please note that at the time this CVE was issued, the policy is an experimental feature of `Node.js`.
- [CVE-2016-5397](#): The Apache Thrift Go client library exposed the potential during code generation for command injection due to using an external formatting tool. Affected Apache Thrift 0.9.3 and older, Fixed in Apache Thrift 0.10.0.
- [CVE-2022-3294](#): Users may have access to secure endpoints in the control plane network. Kubernetes clusters are only affected if an untrusted user can modify Node objects and send proxy requests to them. Kubernetes supports node proxying, which allows clients of `kube-apiserver` to access endpoints of a Kubelet to establish connections to Pods, retrieve container logs, and more. While Kubernetes already validates the proxying address for Nodes, a bug in `kube-apiserver` made it possible to bypass this validation. Bypassing this validation could allow authenticated requests destined for Nodes to to the API server's private network.

- [CVE-2023-46402](#): git-urls 1.0.0 allows ReDOS (Regular Expression Denial of Service) in urls.go.
- [RHSA-2024:2098](#): The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.
- [RHSA-2024:0752](#): The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.
- [CVE-2024-23651](#): BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. Two malicious build steps running in parallel sharing the same cache mounts with subpaths could cause a race condition that can lead to files from the host system being accessible to the build container. The issue has been fixed in v0.12.5. Workarounds include, avoiding using BuildKit frontend from an untrusted source or building an untrusted Dockerfile containing cache mounts with `--mount=type=cache,source=...` options.
- [RHSA-2023:4419](#): OpenSSH is an SSH protocol implementation supported by a number of Linux, UNIX, and similar operating systems. It includes the core files necessary for both the OpenSSH client and server.
- [RHSA-2024:2699](#): Git Large File Storage (LFS) replaces large files such as audio samples, videos, datasets, and graphics with text pointers inside Git, while storing the file contents on a remote server.
- [RHSA-2024:1444](#): Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- [RHSA-2023:5360](#): Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- [RHSA-2023:5850](#): Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- [CVE-2023-43646](#): get-func-name is a module to retrieve a function's name securely and consistently both in NodeJS and the browser. Versions prior to 2.0.1 are subject to a regular expression denial of service (redos) vulnerability which may lead to a denial of service when parsing malicious input. This vulnerability can be exploited when there is an imbalance in parentheses, which results in excessive backtracking and subsequently increases the CPU load and processing time significantly. This vulnerability can be triggered using the following input: `"\t".repeat(54773) + "\t/function/i"`. This issue has been addressed in commit ``f934b228b`` which has been included in releases from 2.0.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.
- [CVE-2023-45133](#): Babel is a compiler for writing JavaScript. In ``@babel/traverse`` prior to versions 7.23.2 and 8.0.0-alpha.4 and all versions of ``babel-traverse``, using Babel to compile code that was specifically crafted by an attacker can lead to arbitrary code execution during compilation, when using plugins that rely on the ``path.evaluate()`` or ``path.evaluateTruthy()`` internal Babel methods. Known affected plugins are ``@babel/plugin-transform-runtime``; ``@babel/preset-env`` when using its ``useBuiltIns`` option; and any "polyfill provider" plugin that depends on ``@babel/helper-define-polyfill-provider``, such as ``babel-plugin-polyfill-corejs3``, ``babel-plugin-polyfill-corejs2``, ``babel-plugin-polyfill-es-shims``, ``babel-plugin-polyfill-regenerator``. No other plugins under the ``@babel/`` namespace are impacted, but third-party plugins might be. Users that only compile trusted code are not impacted. The vulnerability has been fixed in ``@babel/traverse@7.23.2`` and ``@babel/traverse@8.0.0-alpha.4``. Those who cannot upgrade ``@babel/traverse`` and are using one of the affected packages mentioned above should upgrade them to their latest version to avoid triggering the vulnerable code path in affected ``@babel/traverse`` versions: ``@babel/plugin-transform-runtime`` v7.23.2, ``@babel/preset-env`` v7.23.2, ``@babel/helper-define-polyfill-provider`` v0.4.3, ``babel-plugin-polyfill-corejs2`` v0.4.6, ``babel-plugin-polyfill-corejs3`` v0.8.5, ``babel-plugin-polyfill-es-shims`` v0.10.0, ``babel-plugin-polyfill-regenerator`` v0.5.3.
- [CVE-2024-27983](#): An attacker can make the Node.js HTTP/2 server completely unavailable by sending a small amount of HTTP/2 frames packets with a few HTTP/2 frames inside. It is possible to leave some data in nhttp2 memory after reset when headers with HTTP/2 CONTINUATION frame are sent to the server and then a TCP connection is abruptly closed by the client triggering the Http2Session destructor while header frames are still being processed (and stored in memory) causing a race condition.
- [CVE-2021-33910](#): basic/unit-name.c in systemd prior to 246.15, 247.8, 248.5, and 249.1 has a Memory Allocation with an Excessive Size Value (involving `strdupa` and `alloca` for a pathname controlled by a local attacker) that results in an operating system crash.
- [CVE-2023-43665](#): In Django 3.2 before 3.2.22, 4.1 before 4.1.12, and 4.2 before 4.2.6, the `django.utils.text.Truncator.chars()` and `words()` methods (when used with `html=True`) are subject to a potential DoS (denial of service) attack via certain inputs with very long, potentially malformed HTML text. The `chars()`

and words() methods are used to implement the truncatechars_html and truncatewords_html template filters, which are thus also vulnerable. NOTE: this issue exists because of an incomplete fix for CVE-2019-14232.

- [CVE-2023-46695](#): An issue was discovered in Django 3.2 before 3.2.23, 4.1 before 4.1.13, and 4.2 before 4.2.7. The NFKC normalization is slow on Windows. As a consequence, django.contrib.auth.forms.UsernameField is subject to a potential DoS (denial of service) attack via certain inputs with a very large number of Unicode characters.
- [CVE-2023-41164](#): In Django 3.2 before 3.2.21, 4.1 before 4.1.11, and 4.2 before 4.2.5, django.utils.encoding.uri_to_iri() is subject to a potential DoS (denial of service) attack via certain inputs with a very large number of Unicode characters.
- [CVE-2024-24680](#): An issue was discovered in Django 3.2 before 3.2.24, 4.2 before 4.2.10, and Django 5.0 before 5.0.2. The intcomma template filter was subject to a potential denial-of-service attack when used with very long strings.
- [CVE-2022-44570](#): A denial of service vulnerability in the Range header parsing component of Rack >= 1.5.0. A Carefully crafted input can cause the Range header parsing component in Rack to take an unexpected amount of time, possibly resulting in a denial of service attack vector. Any applications that deal with Range requests (such as streaming applications, or applications that serve files) may be impacted.
- [CVE-2023-27530](#): A DoS vulnerability exists in Rack <v3.0.4.2, <v2.2.6.3, <v2.1.4.3 and <v2.0.9.3 within in the Multipart MIME parsing code in which could allow an attacker to craft requests that can be abuse to cause multipart parsing to take longer than expected.
- [CVE-2022-44571](#): There is a denial of service vulnerability in the Content-Disposition parsing component of Rack fixed in 2.0.9.2, 2.1.4.2, 2.2.4.1, 3.0.0.1. This could allow an attacker to craft an input that can cause Content-Disposition header parsing in Rack to take an unexpected amount of time, possibly resulting in a denial of service attack vector. This header is used typically used in multipart parsing. Any applications that parse multipart posts using Rack (virtually all Rails applications) are impacted.
- [CVE-2020-8184](#): A reliance on cookies without validation/integrity check security vulnerability exists in rack < 2.2.3, rack < 2.1.4 that makes it is possible for an attacker to forge a secure or host-only cookie prefix.
- [CVE-2022-44572](#): A denial of service vulnerability in the multipart parsing component of Rack fixed in 2.0.9.2, 2.1.4.2, 2.2.4.1 and 3.0.0.1 could allow an attacker to craft input that can cause RFC2183 multipart boundary parsing in Rack to take an unexpected amount of time, possibly resulting in a denial of service attack vector. Any applications that parse multipart posts using Rack (virtually all Rails applications) are impacted.
- [CVE-2022-30122](#): A possible denial of service vulnerability exists in Rack <2.0.9.1, <2.1.4.1 and <2.2.3.1 in the multipart parsing component of Rack.
- [CVE-2023-28319](#): A use after free vulnerability exists in curl <v8.1.0 in the way libcurl offers a feature to verify an SSH server's public key using a SHA 256 hash. When this check fails, libcurl would free the memory for the fingerprint before it returns an error message containing the (now freed) hash. This flaw risks inserting sensitive heap-based data into the error message that might be shown to users or otherwise get leaked and revealed.
- [CVE-2023-35945](#): Envoy is a cloud-native high-performance edge/middle/service proxy. Envoy's HTTP/2 codec may leak a header map and bookkeeping structures upon receiving `RST_STREAM` immediately followed by the `GOAWAY` frames from an upstream server. In nghttp2, cleanup of pending requests due to receipt of the `GOAWAY` frame skips de-allocation of the bookkeeping structure and pending compressed header. The error return [code path] is taken if connection is already marked for not sending more requests due to `GOAWAY` frame. The clean-up code is right after the return statement, causing memory leak. Denial of service through memory exhaustion. This vulnerability was patched in versions(s) 1.26.3, 1.25.8, 1.24.9, 1.23.11.
- [RHSA-2023:4035](#): Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- [RHSA-2023:5362](#): Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- [RHSA-2023:5869](#): Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- [RHSA-2024:1435](#): PostgreSQL is an advanced object-relational database management system. The postgresql-jdbc package includes the .jar files needed for Java programs to access a PostgreSQL database.
- [CVE-2024-23226](#): The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, tvOS 17.4. Processing web content may lead to arbitrary code execution.

- [CVE-2023-42950](#): A use after free issue was addressed with improved memory management. This issue is fixed in Safari 17.2, iOS 17.2 and iPadOS 17.2, tvOS 17.2, watchOS 10.2, macOS Sonoma 14.2. Processing maliciously crafted web content may lead to arbitrary code execution.
- [RHSA-2024:2126](#): WebKitGTK is the port of the portable web rendering engine WebKit to the GTK platform.
- [CVE-2023-30608](#): sqlparse is a non-validating SQL parser module for Python. In affected versions the SQL parser contains a regular expression that is vulnerable to ReDoS (Regular Expression Denial of Service). This issue was introduced by commit `e75e358`. The vulnerability may lead to Denial of Service (DoS). This issues has been fixed in sqlparse 0.4.4 by commit `c457abd5f`. Users are advised to upgrade. There are no known workarounds for this issue.
- [CVE-2023-6932](#): A use-after-free vulnerability in the Linux kernel's ipv4: igmp component can be exploited to achieve local privilege escalation. A race condition can be exploited to cause a timer be mistakenly registered on a RCU read locked object which is freed by another thread. We recommend upgrading past commit e2b706c691905fe78468c361aaabc719d0a496f1.
- [CVE-2023-6931](#): A heap out-of-bounds write vulnerability in the Linux kernel's Performance Events system component can be exploited to achieve local privilege escalation. A perf_event's read_size can overflow, leading to an heap out-of-bounds increment or write in perf_read_group(). We recommend upgrading past commit 382c27f4ed28f803b1f1473ac2d8db0afc795a1b.
- [CVE-2023-20588](#): A division-by-zero error on some AMD processors can potentially return speculative data resulting in loss of confidentiality.
- [CVE-2023-40590](#): GitPython is a python library used to interact with Git repositories. When resolving a program, Python/Windows look for the current working directory, and after that the PATH environment. GitPython defaults to use the `git` command, if a user runs GitPython from a repo has a `git.exe` or `git` executable, that program will be run instead of the one in the user's `PATH`. This is more of a problem on how Python interacts with Windows systems, Linux and any other OS aren't affected by this. But probably people using GitPython usually run it from the CWD of a repo. An attacker can trick a user to download a repository with a malicious `git` executable, if the user runs/imports GitPython from that directory, it allows the attacker to run any arbitrary commands. There is no fix currently available for windows users, however there are a few mitigations. 1: Default to an absolute path for the git program on Windows, like `C:\\Program Files\\Git\\cmd\\git.EXE` (default git path installation). 2: Require users to set the `GIT_PYTHON_GIT_EXECUTABLE` environment variable on Windows systems. 3: Make this problem prominent in the documentation and advise users to never run GitPython from an untrusted repo, or set the `GIT_PYTHON_GIT_EXECUTABLE` env var to an absolute path. 4: Resolve the executable manually by only looking into the `PATH` environment variable.
- [CVE-2023-32559](#): A privilege escalation vulnerability exists in the experimental policy mechanism in all active release lines: 16.x, 18.x and, 20.x. The use of the deprecated API `process.binding()` can bypass the policy mechanism by requiring internal modules and eventually take advantage of `process.binding('spawn_sync')` run arbitrary code, outside of the limits defined in a `policy.json` file. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.
- [CVE-2023-32006](#): The use of `module.constructor.createRequire()` can bypass the policy mechanism and require modules outside of the policy.json definition for a given module. This vulnerability affects all users using the experimental policy mechanism in all active release lines: 16.x, 18.x, and, 20.x. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.
- [CVE-2023-30585](#): A vulnerability has been identified in the Node.js (.msi version) installation process, specifically affecting Windows users who install Node.js using the .msi installer. This vulnerability emerges during the repair operation, where the `msiexec.exe` process, running under the NT AUTHORITY\\SYSTEM context, attempts to read the %USERPROFILE% environment variable from the current user's registry.

The issue arises when the path referenced by the %USERPROFILE% environment variable does not exist. In such cases, the `msiexec.exe` process attempts to create the specified path in an unsafe manner, potentially leading to the creation of arbitrary folders in arbitrary locations.

The severity of this vulnerability is heightened by the fact that the %USERPROFILE% environment variable in the Windows registry can be modified by standard (or "non-privileged") users. Consequently, unprivileged actors, including malicious entities or trojans, can manipulate the environment variable key to deceive the

privileged `msiexec.exe` process. This manipulation can result in the creation of folders in unintended and potentially malicious locations.

It is important to note that this vulnerability is specific to Windows users who install Node.js using the .msi installer. Users who opt for other installation methods are not affected by this particular issue.

- [CVE-2023-4807](#): Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on the Windows 64 platform when running on newer X86_64 processors supporting the AVX512-IFMA instructions. Impact summary: If in an application that uses the OpenSSL library an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences.

The POLY1305 MAC (message authentication code) implementation in OpenSSL does not save the contents of non-volatile XMM registers on Windows 64 platform when calculating the MAC of data larger than 64 bytes. Before returning to the caller all the XMM registers are set to zero rather than restoring their previous content. The vulnerable code is used only on newer x86_64 processors supporting the AVX512-IFMA instructions.

The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However given the contents of the registers are just zeroed so the attacker cannot put arbitrary values inside, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service.

The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3 and a malicious client can influence whether this AEAD cipher is used by the server. This implies that server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue.

As a workaround the AVX512-IFMA instructions support can be disabled at runtime by setting the environment variable `OPENSSL_ia32cap=OPENSSL_ia32cap:-0x200000`. The FIPS provider is not affected by this issue.

- [CVE-2023-40283](#): An issue was discovered in `l2cap_sock_release` in `net/bluetooth/l2cap_sock.c` in the Linux kernel before 6.4.10. There is a use-after-free because the children of an `sk` are mishandled.
- [CVE-2023-42752](#): An integer overflow flaw was found in the Linux kernel. This issue leads to the kernel allocating `skb_shared_info` in the userspace, which is exploitable in systems without SMAP protection since `skb_shared_info` contains references to function pointers.
- [CVE-2023-1436](#): An infinite recursion is triggered in Jettison when constructing a JSONArray from a Collection that contains a self-reference in one of its elements. This leads to a StackOverflowError exception being thrown.
- [CVE-2022-40149](#): Those using Jettison to parse untrusted XML or JSON data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack.
- [CVE-2022-40150](#): Those using Jettison to parse untrusted XML or JSON data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by Out of memory. This effect may support a denial of service attack.
- [CVE-2022-45685](#): A stack overflow in Jettison before v1.5.2 allows attackers to cause a Denial of Service (DoS) via crafted JSON data.
- [CVE-2022-45693](#): Jettison before v1.5.2 was discovered to contain a stack overflow via the map parameter. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.
- [RHSA-2024:2447](#): OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as a full-strength general-purpose cryptography library.
- [CVE-2020-29562](#): The `iconv` function in the GNU C Library (aka glibc or libc6) 2.30 to 2.32, when converting UCS4 text containing an irreversible character, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.
- [CVE-2021-27645](#): The nameserver caching daemon (nscd) in the GNU C Library (aka glibc or libc6) 2.29 through 2.33, when processing a request for netgroup lookup, may crash due to a double-free, potentially resulting in degraded service or Denial of Service on the local system. This is related to `netgroupcache.c`.

- [CVE-2020-12723](#): regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls.
- [CVE-2020-10878](#): Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.
- [CVE-2020-10543](#): Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
- [CVE-2021-20232](#): A flaw was found in gnutls. A use after free issue in client_send_params in lib/ext/pre_shared_key.c may lead to memory corruption and other potential consequences.
- [CVE-2021-20231](#): A flaw was found in gnutls. A use after free issue in client sending key_share extension may lead to memory corruption and other consequences.
- [CVE-2023-38546](#): This flaw allows an attacker to insert cookies at will into a running program using libcurl, if the specific series of conditions are met. libcurl performs transfers. In its API, an application creates 'easy handles' that are the individual handles for single transfers. libcurl provides a function call that duplicates an easy handle called curl_easy_duphandle. If a transfer has cookies enabled when the handle is duplicated, the cookie-enable state is also cloned - but without cloning the actual cookies. If the source handle did not read any cookies from a specific file on disk, the cloned version of the handle would instead store the file name as none (using the four ASCII letters, no quotes). Subsequent use of the cloned handle that does not explicitly set a source to load cookies from would then inadvertently load cookies from a file named none - if such a file exists and is readable in the current directory of the program using libcurl. And if using the correct file format of course.
- [CVE-2017-7244](#): The _pcre32_xclass function in pcre_xclass.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (invalid memory read) via a crafted file.
- [CVE-2018-16429](#): GNOME GLib 2.56.1 has an out-of-bounds read vulnerability in g_markup_parse_context_parse() in gmarkup.c, related to utf8_str().
- [CVE-2019-13012](#): The keyfile settings backend in GNOME GLib (aka glib2.0) before 2.60.0 creates directories using g_file_make_directory_with_parents (kfsb->dir, NULL, NULL) and files using g_file_replace_contents (kfsb->file, contents, length, NULL, FALSE, G_FILE_CREATE_REPLACE_DESTINATION, NULL, NULL, NULL). Consequently, it does not properly restrict directory (and file) permissions. Instead, for directories, 0777 permissions are used; for files, default file permissions are used. This is similar to CVE-2019-12450.
- [CVE-2021-28153](#): An issue was discovered in GNOME GLib before 2.66.8. When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION to replace a path that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceivably have security relevance if the symlink is attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly remain unchanged.)
- [CVE-2023-2602](#): A vulnerability was found in the pthread_create() function in libcap. This issue may allow a malicious actor to use cause __real_pthread_create() to return an error, which can exhaust the process memory.
- [CVE-2015-2059](#): The stringprep_utf8_to_ucs4 function in libin before 1.31, as used in jabberd2, allows context-dependent attackers to read system memory and possibly have other unspecified impact via invalid UTF-8 characters in a string, which triggers an out-of-bounds read.
- [CVE-2015-8948](#): idn in GNU libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte as input, which triggers an out-of-bounds read.
- [CVE-2017-5969](#): libxml2 2.9.4, when used in recover mode, allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted XML document. NOTE: The maintainer states "I would disagree of a CVE with the Recover parsing option which should only be used for manual recovery at least for XML parser.
- [CVE-2017-8872](#): The htmlParseTryOrFinish function in HTMLparser.c in libxml2 2.9.4 allows attackers to cause a denial of service (buffer over-read) or information disclosure.
- [CVE-2017-9048](#): libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a stack-based buffer overflow. The function xmlSprintfElementContent in valid.c is supposed to recursively dump the element content definition into a char buffer 'buf' of size 'size'. At the end of the routine, the function may strcat two more characters without checking whether the current strlen(buf) + 2 < size. This vulnerability causes programs that use libxml2, such as PHP, to crash.
- [CVE-2016-4984](#): /usr/libexec/openssl/generate-server-cert.sh in openssl-servers sets weak permissions for the TLS certificate, which allows local users to obtain the TLS certificate by leveraging a race condition between the creation of the certificate, and the chmod to protect it.

- [CVE-2017-11462](#): Double free vulnerability in MIT Kerberos 5 (aka krb5) allows attackers to have unspecified impact via vectors involving automatic deletion of security contexts on error.
- [CVE-2016-8621](#): The ``curl_getdate`` function in curl before version 7.51.0 is vulnerable to an out of bounds read if it receives an input with one digit short.
- [CVE-2016-8622](#): The URL percent-encoding decode function in libcurl before 7.51.0 is called ``curl_easy_unescape``. Internally, even if this function would be made to allocate a unescape destination buffer larger than 2GB, it would return that new length in a signed 32 bit integer variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer.
- [CVE-2016-8623](#): A flaw was found in curl before version 7.51.0. The way curl handles cookies permits other threads to trigger a use-after-free leading to information disclosure.
- [CVE-2021-3200](#): Buffer overflow vulnerability in libsolv 2020-12-13 via the Solver * testcase_read(Pool *pool, FILE *fp, const char *testcase, Queue *job, char **resultp, int *resultflagsp function at src/testcase.c: line 2334, which could cause a denial of service
- [CVE-2016-9586](#): curl before version 7.52.0 is vulnerable to a buffer overflow when doing a large floating point output in libcurl's implementation of the printf() functions. If there are any application that accepts a format string from the outside without necessary input filtering, it could allow remote attacks.
- [CVE-2017-1000100](#): When doing a TFTP transfer and curl/libcurl is given a URL that contains a very long file name (longer than about 515 bytes), the file name is truncated to fit within the buffer boundaries, but the buffer size is still wrongly updated to use the untruncated length. This too large value is then used in the sendto() call, making curl attempt to send more data than what is actually put into the buffer. The endto() function will then read beyond the end of the heap based buffer. A malicious HTTP(S) server could redirect a vulnerable libcurl-using client to a crafted TFTP URL (if the client hasn't restricted which protocols it allows redirects to) and trick it to send private memory contents to a remote server over UDP. Limit curl's redirect protocols with --proto-redir and libcurl's with CURLOPT_REDIR_PROTOCOLS.
- [CVE-2021-37621](#): Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An infinite loop was found in Exiv2 versions v0.27.4 and earlier. The infinite loop is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the image ICC profile, which is a less frequently used Exiv2 operation that requires an extra command line option (``-p C``). The bug is fixed in version v0.27.5.
- [CVE-2021-37620](#): Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 versions v0.27.4 and earlier. The out-of-bounds read is triggered when Exiv2 is used to read the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. The bug is fixed in version v0.27.5.
- [CVE-2021-37616](#): Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A null pointer dereference was found in Exiv2 versions v0.27.4 and earlier. The null pointer dereference is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the interpreted (translated) data, which is a less frequently used Exiv2 operation that requires an extra command line option (``-p t`` or ``-P t``). The bug is fixed in version v0.27.5.
- [CVE-2021-34335](#): Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A floating point exception (FPE) due to an integer divide by zero was found in Exiv2 versions v0.27.4 and earlier. The FPE is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the interpreted (translated) data, which is a less frequently used Exiv2 operation that requires an extra command line option (``-p t`` or ``-P t``). The bug is fixed in version v0.27.5.
- [CVE-2021-37623](#): Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An infinite loop was found in Exiv2 versions v0.27.4 and earlier. The infinite loop is triggered when Exiv2 is used to modify the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted

image file. Note that this bug is only triggered when deleting the IPTC data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-d I rm``). The bug is fixed in version v0.27.5.

- [CVE-2021-34334](#): Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An infinite loop is triggered when Exiv2 is used to read the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. The bug is fixed in version v0.27.5.
- [CVE-2021-32815](#): Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. The assertion failure is triggered when Exiv2 is used to modify the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when modifying the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as ``fi``.
Patches The bug is fixed in version v0.27.5. ### References Regression test and bug fix: #1739 ### For more information Please see our [security policy](#) for information about Exiv2 security.
- [CVE-2021-37622](#): Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An infinite loop was found in Exiv2 versions v0.27.4 and earlier. The infinite loop is triggered when Exiv2 is used to modify the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when deleting the IPTC data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-d I rm``). The bug is fixed in version v0.27.5.
- [CVE-2020-18771](#): Exiv2 0.27.99.0 has a global buffer over-read in `Exiv2::Internal::Nikon1MakerNote::print0x0088` in `nikonmn_int.cpp` which can result in an information leak.
- [CVE-2021-37615](#): Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A null pointer dereference was found in Exiv2 versions v0.27.4 and earlier. The null pointer dereference is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the interpreted (translated) data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-p t`` or `-P t``). The bug is fixed in version v0.27.5.
- [CVE-2018-13419](#): An issue has been found in `libsndfile 1.0.28`. There is a memory leak in `psf_allocate` in `common.c`, as demonstrated by `sndfile-convert`. NOTE: The maintainer and third parties were unable to reproduce and closed the issue
- [CVE-2023-4132](#): A use-after-free vulnerability was found in the `siano smsusb` module in the Linux kernel. The bug occurs during device initialization when the `siano` device is plugged in. This flaw allows a local user to crash the system, causing a denial of service condition.
- [CVE-2021-41617](#): `sshd` in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for `AuthorizedKeysCommand` and `AuthorizedPrincipalsCommand` may run with privileges associated with group memberships of the `sshd` process, if the configuration specifies running the command as a different user.
- [CVE-2023-35827](#): An issue was discovered in the Linux kernel through 6.3.8. A use-after-free was found in `ravb_remove` in `drivers/net/ethernet/renesas/ravb_main.c`.
- [CVE-2023-3212](#): A NULL pointer dereference issue was found in the `gfs2` file system in the Linux kernel. It occurs on corrupt `gfs2` file systems when the `evict` code tries to reference the journal descriptor structure after it has been freed and set to NULL. A privileged local user could use this flaw to cause a kernel panic.
- [CVE-2022-3162](#): Users authorized to list or watch one type of namespaced custom resource cluster-wide can read custom resources of a different type in the same API group without authorization. Clusters are impacted by this vulnerability if all of the following are true: 1. There are 2+ `CustomResourceDefinitions` sharing the same API group 2. Users have cluster-wide list or watch authorization on one of those custom resources. 3. The same users are not authorized to read another custom resource in the same API group.
- [RHSAs-2023:3042](#): GNU Emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a scripting language (`elisp`), and the capability to read e-mail and news.
- [RHSAs-2024:0606](#): OpenSSH is an SSH protocol implementation supported by a number of Linux, UNIX, and similar operating systems. It includes the core files necessary for both the OpenSSH client and server.

- [CVE-2024-23650](#): BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. A malicious BuildKit client or frontend could craft a request that could lead to BuildKit daemon crashing with a panic. The issue has been fixed in v0.12.5. As a workaround, avoid using BuildKit frontends from untrusted sources.
- [RHSA-2023:2758](#): The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.
- [RHSA-2023:6939](#): The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.
- [RHSA-2023:2866](#): Git Large File Storage (LFS) replaces large files such as audio samples, videos, datasets, and graphics with text pointers inside Git, while storing the file contents on a remote server.
- [CVE-2024-22025](#): A vulnerability in Node.js has been identified, allowing for a Denial of Service (DoS) attack through resource exhaustion when using the `fetch()` function to retrieve content from an untrusted URL.

The vulnerability stems from the fact that the `fetch()` function in Node.js always decodes Brotli, making it possible for an attacker to cause resource exhaustion when fetching content from an untrusted URL.

An attacker controlling the URL passed into `fetch()` can exploit this vulnerability to exhaust memory, potentially leading to process termination, depending on the system configuration.

- [CVE-2022-29244](#): `npm pack` ignores root-level `.gitignore` and `.npmignore` file exclusion directives when run in a workspace or with a workspace flag (ie. `--workspaces`, `--workspace=<name>`). Anyone who has run ``npm pack`` or ``npm publish`` inside a workspace, as of v7.9.0 and v7.13.0 respectively, may be affected and have published files into the npm registry they did not intend to include. Users should upgrade to the latest, patched version of npm v8.11.0, run: `npm i -g npm@latest`. Node.js versions v16.15.1, v17.19.1, and v18.3.0 include the patched v8.11.0 version of npm.
- [CVE-2023-46809](#): A flaw was found in Node.js. The `privateDecrypt()` API of the `crypto` library may allow a covert timing side-channel during PKCS#1 v1.5 padding error handling. This issue revealed significant timing differences in decryption for valid and invalid ciphertexts, which may allow a remote attacker to decrypt captured RSA ciphertexts or forge signatures, especially in scenarios involving API endpoints processing JSON Web Encryption messages.
- [CVE-2024-27982](#): The team has identified a critical vulnerability in the http server of the most recent version of Node, where malformed headers can lead to HTTP request smuggling. Specifically, if a space is placed before a content-length header, it is not interpreted correctly, enabling attackers to smuggle in a second request within the body of the first.
- [CVE-2024-29041](#): Express.js minimalist web framework for node. Versions of Express.js prior to 4.19.0 and all pre-release alpha and beta versions of 5.0 are affected by an open redirect vulnerability using malformed URLs. When a user of Express performs a redirect using a user-provided URL Express performs an encode [using ``encodeURIComponent``] (<https://github.com/pillarjs/encodeURIComponent>) on the contents before passing it to the ``location`` header. This can cause malformed URLs to be evaluated in unexpected ways by common redirect allow list implementations in Express applications, leading to an Open Redirect via bypass of a properly implemented allow list. The main method impacted is ``res.location()`` but this is also called from within ``res.redirect()``. The vulnerability is fixed in 4.19.2 and 5.0.0-beta.3.
- [RHSA-2023:7747](#): The `libxml2` library is a development toolbox providing the implementation of various XML standards.
- [RHSA-2024:0463](#): The RPM Package Manager (RPM) is a command-line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.
- [RHSA-2024:0465](#): SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file. The API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of an SQL database without the administrative hassles of supporting a separate database server.
- [RHSA-2024:2438](#): Pluggable Authentication Modules (PAM) provide a system to set up authentication policies without the need to recompile programs to handle authentication.
- [CVE-2020-29363](#): An issue was discovered in p11-kit 0.23.6 through 0.23.21. A heap-based buffer overflow has been discovered in the RPC protocol used by p11-kit server/remote commands and the client library. When the remote entity supplies a serialized byte array in a `CK_ATTRIBUTE`, the receiving entity may not allocate sufficient length for the buffer to store the deserialized value.

- [CVE-2020-27350](#): APT had several integer overflows and underflows while parsing .deb packages, aka GHSL-2020-168 GHSL-2020-169, in files apt-pkg/contrib/extracttar.cc, apt-pkg/deb/debfile.cc, and apt-pkg/contrib/arfile.cc. This issue affects: apt 1.2.32ubuntu0 versions prior to 1.2.32ubuntu0.2; 1.6.12ubuntu0 versions prior to 1.6.12ubuntu0.2; 2.0.2ubuntu0 versions prior to 2.0.2ubuntu0.2; 2.1.10ubuntu0 versions prior to 2.1.10ubuntu0.1;
- [CVE-2020-24659](#): An issue was discovered in GnuTLS before 3.6.15. A server can trigger a NULL pointer dereference in a TLS 1.3 client if a no_renegotiation alert is sent with unexpected timing, and then an invalid second handshake occurs. The crash happens in the application's error handling path, where the gnutls_deinit function is called after detecting a handshake failure.
- [CVE-2023-32360](#): An authentication issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7.7, macOS Monterey 12.6.6, macOS Ventura 13.4. An unauthenticated user may be able to access recently printed documents.
- [CVE-2023-34241](#): OpenPrinting CUPS is a standards-based, open source printing system for Linux and other Unix-like operating systems. Starting in version 2.0.0 and prior to version 2.4.6, CUPS logs data of free memory to the logging service AFTER the connection has been closed, when it should have logged the data right before. This is a use-after-free bug that impacts the entire cupsd process.

The exact cause of this issue is the function `httpClose(con->http)` being called in `scheduler/client.c`. The problem is that `httpClose` always, provided its argument is not null, frees the pointer at the end of the call, only for `cupsdLogClient` to pass the pointer to `httpGetHostname`. This issue happens in function `cupsdAcceptClient` if `LogLevel` is warn or higher and in two scenarios: there is a double-lookup for the IP Address (`HostNameLookups Double` is set in `cupsd.conf`) which fails to resolve, or if CUPS is compiled with TCP wrappers and the connection is refused by rules from `/etc/hosts.allow` and `/etc/hosts.deny`.

Version 2.4.6 has a patch for this issue.

- [CVE-2021-3995](#): A logic error was found in the libmount library of util-linux in the function that allows an unprivileged user to unmount a FUSE filesystem. This flaw allows an unprivileged local attacker to unmount FUSE filesystems that belong to certain other users who have a UID that is a prefix of the UID of the attacker in its string form. An attacker may use this flaw to cause a denial of service to applications that use the affected filesystems.
- [CVE-2021-3996](#): A logic error was found in the libmount library of util-linux in the function that allows an unprivileged user to unmount a FUSE filesystem. This flaw allows a local user on a vulnerable system to unmount other users' filesystems that are either world-writable themselves (like /tmp) or mounted in a world-writable directory. An attacker may use this flaw to cause a denial of service to applications that use the affected filesystems.
- [CVE-2023-3138](#): A vulnerability was found in libX11. The security flaw occurs because the functions in `src/InitExt.c` in libX11 do not check that the values provided for the Request, Event, or Error IDs are within the bounds of the arrays that those functions write to, using those IDs as array indexes. They trust that they were called with values provided by an Xserver adhering to the bounds specified in the X11 protocol, as all X servers provided by X.Org do. As the protocol only specifies a single byte for these values, an out-of-bounds value provided by a malicious server (or a malicious proxy-in-the-middle) can only overwrite other portions of the Display structure and not write outside the bounds of the Display structure itself, possibly causing the client to crash with this memory corruption.
- [CVE-2021-20305](#): A flaw was found in Nettle in versions before 3.7.2, where several Nettle signature verification functions (GOST DSA, EDDSA & ECDSA) result in the Elliptic Curve Cryptography point (ECC) multiply function being called with out-of-range scalars, possibly resulting in incorrect results. This flaw allows an attacker to force an invalid signature, causing an assertion failure or possible validation. The highest threat to this vulnerability is to confidentiality, integrity, as well as system availability.
- [CVE-2021-3580](#): A flaw was found in the way nettle's RSA decryption functions handled specially crafted ciphertext. An attacker could use this flaw to provide a manipulated ciphertext leading to application crash and denial of service.
- [CVE-2021-24031](#): In the Zstandard command-line utility prior to v1.4.1, output files were created with default permissions. Correct file permissions (matching the input) would only be set at completion time. Output files could therefore be readable or writable to unintended parties.
- [CVE-2023-22045](#): Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java

SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).

- [CVE-2023-22049](#): Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
- [RHSA-2023:7034](#): Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems.
- [CVE-2023-49081](#): aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Improper validation made it possible for an attacker to modify the HTTP request (e.g. to insert a new header) or create a new HTTP request if the attacker controls the HTTP version. The vulnerability only occurs if the attacker can control the HTTP version of the request. This issue has been patched in version 3.9.0.
- [CVE-2024-23829](#): aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Security-sensitive parts of the Python HTTP parser retained minor differences in allowable character sets, that must trigger error handling to robustly match frame boundaries of proxies in order to protect against injection of additional requests. Additionally, validation could trigger exceptions that were not handled consistently with processing of other malformed input. Being more lenient than internet standards require could, depending on deployment environment, assist in request smuggling. The unhandled exception could cause excessive resource consumption on the application server and/or its logging facilities. This vulnerability exists due to an incomplete fix for CVE-2023-47627. Version 3.9.2 fixes this vulnerability.
- [CVE-2023-49082](#): aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Improper validation makes it possible for an attacker to modify the HTTP request (e.g. insert a new header) or even create a new HTTP request if the attacker controls the HTTP method. The vulnerability occurs only if the attacker can control the HTTP method (GET, POST etc.) of the request. If the attacker can control the HTTP version of the request it will be able to modify the request (request smuggling). This issue has been patched in version 3.9.0.
- [CVE-2024-25629](#): c-ares is a C library for asynchronous DNS requests. `ares__read_line()` is used to parse local configuration files such as `/etc/resolv.conf`, `/etc/nsswitch.conf`, the `HOSTALIASES` file, and if using a c-ares version prior to 1.27.0, the `/etc/hosts` file. If any of these configuration files has an embedded `NULL` character as the first character in a new line, it can lead to attempting to read memory prior to the start of the given buffer which may result in a crash. This issue is fixed in c-ares 1.27.0. No known workarounds exist.
- [CVE-2023-23916](#): An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP compression algorithms, meaning that a server response can be compressed multiple times and potentially with differential algorithms. The number of acceptable "links" in this "decompression chain" was capped, but the cap was implemented on a per-header basis allowing a malicious server to insert a virtually unlimited number of compression steps simply by using many headers. The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying to and returning out of memory errors.

- [CVE-2023-27537](#): A double free vulnerability exists in libcurl <8.0.0 when sharing HSTS data between separate "handles". This sharing was introduced without considerations for do this sharing across separate threads but there was no indication of this fact in the documentation. Due to missing mutexes or thread locks, two threads sharing the same HSTS data could end up doing a double-free or use-after-free.
- [CVE-2018-1002104](#): Versions < 1.5 of the Kubernetes ingress default backend, which handles invalid ingress traffic, exposed prometheus metrics publicly.
- [DSA-5686-1](#): dav1d - security update
- [RHSA-2024:1530](#): Expat is a C library for parsing XML documents.
- [RHSA-2023:1583](#): Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- [RHSA-2023:4536](#): Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- [RHSA-2022:1830](#): PostgreSQL is an advanced object-relational database management system (DBMS).
- [CVE-2021-3782](#): An internal reference count is held on the buffer pool, incremented every time a new buffer is created from the pool. The reference count is maintained as an int; on LP64 systems this can cause the reference count to overflow if the client creates a large number of wl_shm buffer objects, or if it can coerce the server to create a large number of external references to the buffer storage. With the reference count overflowing, a use-after-free can be constructed on the wl_shm_pool tracking structure, where values may be incremented or decremented; it may also be possible to construct a limited oracle to leak 4 bytes of server-side memory to the attacking client at a time.
- [CVE-2020-36023](#): An issue was discovered in freedesktop poppler version 20.12.1, allows remote attackers to cause a denial of service (DoS) via crafted .pdf file to FoFiType1C::cvtGlyph function.
- [CVE-2020-36024](#): An issue was discovered in freedesktop poppler version 20.12.1, allows remote attackers to cause a denial of service (DoS) via crafted .pdf file to FoFiType1C::convertToType1 function.
- [CVE-2022-37050](#): In Poppler 22.07.0, PDFDoc::savePageAs in PDFDoc.c allows attackers to cause a denial-of-service (application crashes with SIGABRT) by crafting a PDF file in which the xref data structure is mishandled in getCatalog processing. Note that this vulnerability is caused by the incomplete patch of CVE-2018-20662.
- [CVE-2022-37051](#): An issue was discovered in Poppler 22.07.0. There is a reachable abort which leads to denial of service because the main function in pdfunite.cc lacks a stream check before saving an embedded file.
- [CVE-2022-37052](#): A reachable Object::getString assertion in Poppler 22.07.0 allows attackers to cause a denial of service due to a failure in markObject.
- [RHSA-2024:2302](#): GStreamer is a streaming media framework based on graphs of filters which operate on media data. The gstreamer1-plugins-base packages contain a collection of well-maintained base plug-ins.
- [RHSA-2024:2295](#): The libjpeg-turbo packages contain a library of functions for manipulating JPEG images. They also contain simple client programs for accessing the libjpeg functions. These packages provide the same functionality and API as libjpeg but with better performance.
- [RHSA-2024:2184](#): libsndfile is a C library for reading and writing files containing sampled sound, such as AIFF, AU, or WAV.
- [RHSA-2024:2410](#): HarfBuzz is an implementation of the OpenType Layout engine.
- [CVE-2023-42843](#): An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1, Safari 17.1, macOS Sonoma 14.1. Visiting a malicious website may lead to address bar spoofing.
- [CVE-2023-42956](#): The issue was addressed with improved memory handling. This issue is fixed in Safari 17.2, iOS 17.2 and iPadOS 17.2, macOS Sonoma 14.2. Processing web content may lead to a denial-of-service.
- [CVE-2024-23252](#): Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
- [CVE-2024-23254](#): The issue was addressed with improved UI handling. This issue is fixed in tvOS 17.4, macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, Safari 17.4. A malicious website may exfiltrate audio data cross-origin.
- [CVE-2024-23263](#): A logic issue was addressed with improved validation. This issue is fixed in tvOS 17.4, macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, iOS 16.7.6 and iPadOS 16.7.6, Safari 17.4. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.

- [CVE-2024-23280](#): An injection issue was addressed with improved validation. This issue is fixed in Safari 17.4, macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, watchOS 10.4, tvOS 17.4. A maliciously crafted webpage may be able to fingerprint the user.
- [CVE-2024-23284](#): A logic issue was addressed with improved state management. This issue is fixed in tvOS 17.4, macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, iOS 16.7.6 and iPadOS 16.7.6, Safari 17.4. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.
- [RHSA-2024:2145](#): The libX11 packages contain the core X11 protocol client library.
- [RHSA-2024:2433](#): Avahi is an implementation of the DNS Service Discovery and Multicast DNS specifications for Zero Configuration Networking. It facilitates service discovery on a local network. Avahi and Avahi-aware applications allow you to plug your computer into a network and, with no configuration, view other people to chat with, view printers to print with, and find shared files on other computers.
- [RHSA-2024:2289](#): The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.
- [RHSA-2023:2867](#): PostgreSQL is an advanced object-relational database management system. The postgresql-jdbc package includes the .jar files needed for Java programs to access a PostgreSQL database.
- [CVE-2022-21724](#): pgjdbc is the official PostgreSQL JDBC Driver. A security hole was found in the jdbc driver for postgresql database while doing security research. The system using the postgresql library will be attacked when attacker control the jdbc url or properties. pgjdbc instantiates plugin instances based on class names provided via `authenticationPluginClassName`, `sslhostnamerverifier`, `socketFactory`, `sslfactory`, `sslpasswordcallback` connection properties. However, the driver did not verify if the class implements the expected interface before instantiating the class. This can lead to code execution loaded via arbitrary classes. Users using plugins are advised to upgrade. There are no known workarounds for this issue.
- [CVE-2023-1206](#): A hash collision flaw was found in the IPv6 connection lookup table in the Linux kernel's IPv6 functionality when a user makes a new kind of SYN flood attack. A user located in the local network or with a high bandwidth connection can increase the CPU usage of the server that accepts IPV6 connections up to 95%.
- [CVE-2023-3338](#): A null pointer dereference flaw was found in the Linux kernel's DECnet networking protocol. This issue could allow a remote user to crash the system.
- [CVE-2023-34319](#): The fix for XSA-423 added logic to Linux'es netback driver to deal with a frontend splitting a packet in a way such that not all of the headers would come in one piece. Unfortunately the logic introduced there didn't account for the extreme case of the entire packet being split into as many pieces as permitted by the protocol, yet still being smaller than the area that's specially dealt with to keep all (possible) headers together. Such an unusual packet would therefore trigger a buffer overrun in the driver.
- [CVE-2023-34324](#): Closing of an event channel in the Linux kernel can result in a deadlock. This happens when the close is being performed in parallel to an unrelated Xen console action and the handling of a Xen console interrupt in an unprivileged guest.

The closing of an event channel is e.g. triggered by removal of a paravirtual device on the other side. As this action will cause console messages to be issued on the other side quite often, the chance of triggering the deadlock is not neglectable.

Note that 32-bit Arm-guests are not affected, as the 32-bit Linux kernel on Arm doesn't use queued-RW-locks, which are required to trigger the issue (on Arm32 a waiting writer doesn't block further readers to get the lock).

- [CVE-2023-3863](#): A use-after-free flaw was found in `nfc_llcp_find_local` in `net/nfc/llcp_core.c` in NFC in the Linux kernel. This flaw allows a local user with special privileges to impact a kernel information leak issue.
- [CVE-2023-4194](#): A flaw was found in the Linux kernel's TUN/TAP functionality. This issue could allow a local user to bypass network filters and gain unauthorized access to some resources. The original patches fixing CVE-2023-1076 are incorrect or incomplete. The problem is that the following upstream commits - `a096ccca6e50` ("tun: `tun_chr_open()`: correctly initialize socket uid"), - `66b2c338adce` ("tap: `tap_open()`: correctly initialize socket uid"), pass "`inode->i_uid`" to `sock_init_data_uid()` as the last parameter and that turns out to not be accurate.
- [CVE-2023-3341](#): The code that processes control channel messages sent to `named` calls certain functions recursively during packet parsing. Recursion depth is only limited by the maximum accepted packet size; depending on the environment, this may cause the packet-parsing code to run out of available stack memory, causing `named` to terminate unexpectedly. Since each incoming control channel message is fully parsed before

its contents are authenticated, exploiting this flaw does not require the attacker to hold a valid RNDC key; only network access to the control channel's configured TCP port is necessary.

This issue affects BIND 9 versions 9.2.0 through 9.16.43, 9.18.0 through 9.18.18, 9.19.0 through 9.19.16, 9.9.3-S1 through 9.16.43-S1, and 9.18.0-S1 through 9.18.18-S1.

- **CVE-2021-4001**: A race condition was found in the Linux kernel's eBPF verifier between `bpf_map_update_elem` and `bpf_map_freeze` due to a missing lock in `kernel/bpf/syscall.c`. In this flaw, a local user with a special privilege (`cap_sys_admin` or `cap_bpf`) can modify the frozen mapped address space. This flaw affects kernel versions prior to 5.16 rc2.
- **CVE-2021-46174**: Heap-based Buffer Overflow in function `bfd_getl32` in Binutils `objdump` 3.37.
- **CVE-2022-35205**: An issue was discovered in Binutils `readelf` 2.38.50, reachable assertion failure in function `display_debug_names` allows attackers to cause a denial of service.
- **CVE-2022-44840**: Heap buffer overflow vulnerability in binutils `readelf` before 2.40 via function `find_section_in_set` in file `readelf.c`.
- **CVE-2022-45703**: Heap buffer overflow vulnerability in binutils `readelf` before 2.40 via function `display_debug_section` in file `readelf.c`.
- **CVE-2022-47008**: An issue was discovered function `make_tmpdir`, and `make_tmpname` in `bucomm.c` in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks.
- **CVE-2020-19726**: An issue was discovered in binutils `libbfd.c` 2.36 relating to the auxiliary symbol data allows attackers to read or write to system memory or cause a denial of service.
- **CVE-2023-51385**: In `ssh` in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.
- **CVE-2023-41040**: GitPython is a python library used to interact with Git repositories. In order to resolve some git references, GitPython reads files from the ``.git`` directory, in some places the name of the file being read is provided by the user, GitPython doesn't check if this file is located outside the ``.git`` directory. This allows an attacker to make GitPython read any file from the system. This vulnerability is present in <https://github.com/gitpython-developers/GitPython/blob/1c8310d7cae144f74a671cbe17e51f63a830adbf/git/refs/symbolic.py#L174-L175>. That code joins the base directory with a user given string without checking if the final path is located outside the base directory. This vulnerability cannot be used to read the contents of files but could in theory be used to trigger a denial of service for the program. This issue has not yet been addressed.
- **CVE-2023-5178**: A use-after-free vulnerability was found in `drivers/nvme/target/tcp.c`` in ``nvmet_tcp_free_crypto`` due to a logical bug in the NVMe/TCP subsystem in the Linux kernel. This issue may allow a malicious user to cause a use-after-free and double-free problem, which may permit remote code execution or lead to local privilege escalation.
- **CVE-2023-5717**: A heap out-of-bounds write vulnerability in the Linux kernel's Linux Kernel Performance Events (perf) component can be exploited to achieve local privilege escalation.

If `perf_read_group()` is called while an event's `sibling_list` is smaller than its child's `sibling_list`, it can increment or write to memory locations outside of the allocated buffer.

We recommend upgrading past commit `32671e3799ca2e4590773fd0e63aaa4229e50c06`.

- **CVE-2018-25091**: `urllib3` before 1.24.2 does not remove the authorization HTTP header when following a cross-origin redirect (i.e., a redirect that differs in host, port, or scheme). This can allow for credentials in the authorization header to be exposed to unintended hosts or transmitted in cleartext. Note: this issue exists because of an incomplete fix for CVE-2018-20060 (which was case-sensitive).
- **CVE-2023-38552**: When the Node.js policy feature checks the integrity of a resource against a trusted manifest, the application can intercept the operation and return a forged checksum to the node's policy implementation, thus effectively disabling the integrity check.
- **Impacts**: This vulnerability affects all users using the experimental policy mechanism in all active release lines: 18.x and 20.x. Note that at the time this CVE was issued, the policy mechanism is an experimental feature of Node.js.
- **CVE-2019-15847**: The POWER9 backend in GNU Compiler Collection (GCC) before version 10 could optimize multiple calls of the `__builtin_darn` intrinsic into a single call, thus reducing the entropy of the random number generator. This occurred because a volatile operation was not specified. For example, within a single execution of a program, the output of every `__builtin_darn()` call may be the same.

- [CVE-2018-13410](#): An issue was discovered IW44Image.cpp in djvulibre 3.5.28 in allows attackers to cause a denial of service via divide by zero.
- [CVE-2021-46312](#): An issue was discovered IW44EncodeCodec.cpp in djvulibre 3.5.28 in allows attackers to cause a denial of service via divide by zero.
- [CVE-2021-31239](#): An issue found in SQLite SQLite3 v.3.35.4 that allows a remote attacker to cause a denial of service via the appendvfs.c function.
- [CVE-2021-45346](#): A Memory Leak vulnerability exists in SQLite Project SQLite3 3.35.1 and 3.37.0 via maliciously crafted SQL Queries (made via editing the Database File), it is possible to query a record, and leak subsequent bytes of memory that extend beyond the record, which could let a malicious user obtain sensitive information. NOTE: The developer disputes this as a vulnerability stating that If you give SQLite a corrupted database file and submit a query against the database, it might read parts of the database that you did not intend or expect.
- [CVE-2023-32570](#): VideoLAN dav1d before 1.2.0 has a thread_task.c race condition that can lead to an application crash, related to dav1d_decode_frame_exit.
- TEMP-0841856-B18BAF
- [CVE-2018-13410](#): Info-ZIP Zip 3.0, when the -T and -TT command-line options are used, allows attackers to cause a denial of service (invalid free and application crash) or possibly have unspecified other impact because of an off-by-one error. NOTE: it is unclear whether there are realistic scenarios in which an untrusted party controls the -TT value, given that the entire purpose of -TT is execution of arbitrary commands
- [CVE-2024-28757](#): libexpat through 2.6.1 allows an XML Entity Expansion attack when there is isolated use of external parsers (created via XML_ExternalEntityParserCreate).
- [CVE-2012-0039](#): GLib 2.31.8 and earlier, when the g_str_hash function is used, computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table. NOTE: this issue may be disputed by the vendor; the existence of the g_str_hash function is not a vulnerability in the library, because callers of g_hash_table_new and g_hash_table_new_full can specify an arbitrary hash function that is appropriate for the application.
- [CVE-2022-2817](#): Use After Free in GitHub repository vim/vim prior to 9.0.0213.
- [CVE-2022-2862](#): Use After Free in GitHub repository vim/vim prior to 9.0.0221.
- [CVE-2022-2874](#): NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.0224.
- [CVE-2022-2889](#): Use After Free in GitHub repository vim/vim prior to 9.0.0225.
- [CVE-2022-2982](#): Use After Free in GitHub repository vim/vim prior to 9.0.0260.
- [CVE-2022-3016](#): Use After Free in GitHub repository vim/vim prior to 9.0.0286.
- [CVE-2022-3099](#): Use After Free in GitHub repository vim/vim prior to 9.0.0360.
- [CVE-2022-3134](#): Use After Free in GitHub repository vim/vim prior to 9.0.0389.
- [CVE-2014-8166](#): The browsing feature in the server in CUPS does not filter ANSI escape sequences from shared printer names, which might allow remote attackers to execute arbitrary code via a crafted printer name.

Cumulative hotfixes

The cumulative hotfixes that have been shipped for Cloudera Private Cloud Data Services 1.5.4-CHF1.

CDP Private Cloud Data Services 1.5.4-CHF1

The cumulative hotfixes for new features, known issues, and fixed issues for 1.5.4-CHF1.



Note: ECS Customers: Direct upgrade path is not available. Customers must upgrade to CDP Private Cloud Data Services 1.5.4 prior to consuming any CHF built on top of 1.5.4.

**Note:**

OCP Customers: Direct upgrade path is available. Customers can directly upgrade from CDP Private Cloud Data Services 1.5.2 to any 1.5.4 CHF's.

Whats new in CDP Private Cloud Data Services 1.5.4-CHF1

New features introduced in this cumulative hotfix release of CDP Private Cloud Data Services 1.5.4-CHF1.



Note: Cloudera Manager 7.11.3 CHF7 Data Services (version: 7.11.3.14) support CDP Private Cloud Data Services 1.5.4 CHF1 release.



Note: Cloudera Manager 7.11.3 CHF8 does not support any CDP Private Cloud Data Services release.

Restore CP namespaces independently from system-generated DRS backups

Enhancements to the system-generated DRS backups:

- System-generated backups in DRS are automatic, periodic backups that include control plane and data services' namespaces.
- Through Private Cloud Data Services 1.5.4 release, restoring a system-generated backup from the private cloud management console UI restores all the namespaces present in the backup.
- With this change, such a restore action independently restores only control plane namespaces that are present in the backup.

Known Issues in CDP Private Cloud Data Services 1.5.4-CHF1

There are no new known issues in the 1.5.4 cumulative hotfix CHF1 release of CDP Private Cloud Data Services.

DOCS-21084/DSE-36967 - Namespace Termination issue when using Portworx storage

There is an issue with Portworx version lower than 3.1.1, as the namespace deletion gets stuck in terminating state. Portworx is not able to cleanly unmount and clean up the underlying resources.

The issue is fixed with Portworx version 3.1.1. Upgrade to Portworx version 3.1.1 or to later versions.

Fixed Issues in CDP Private Cloud Data Services 1.5.4-CHF1

The fixes in this cumulative hotfix release of CDP Private Cloud Data Services 1.5.4-CHF1.

OPSX-5104: Cluster Ingress Controller improvements for CML workloads scaling

Customers may experience performance degradation when a large number of CML workload sessions are launched simultaneously, which may result in session timeouts. Customer creates a large amount of CML sessions in a short period of time.

The fix does not need user intervention. The fix added cluster ingress improvements for CML workload scaling.

OPSX-5147: OOM when retrieving size of Binary File

Diagnostics bundle collection no longer fails due to OOM errors.

OPSX-5148: Diagnostics Collection from UI w/ Default No Time Limit Should Not Invoke Timestamp Filtering

The diagnostics collection triggered through the UI, with the default "No Time Limit selected", no longer filters logs by timestamp.

Repository Locations for 1.5.4-CHF1


The URLs for CDP Private Cloud Data Services 1.5.4-CHF1 are listed in the following table:

URL Type	Repository Location
Index	<code>https://username:password@archive.cloudera.com/p/cdp-pvc-ds/1.5.4-h2/</code>
Manifest	Repository: <code>https://username:password@archive.cloudera.com/p/cdp-pvc-ds/1.5.4-h2/manifest.json</code>
Parcels	Repository: <code>https://username:password@archive.cloudera.com/p/cdp-pvc-ds/1.5.4-h2/parcels/</code>

Fixed Common Vulnerabilities and Exposures in 1.5.4 CHF1

Review the Common vulnerabilities and Exposures (CVEs) that were fixed in 1.5.4 CHF1 release of CDP Private Cloud Data Services.

Issue ID	Description
CVE-2004-0230	TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection queue exhaustion) by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections.
CVE-2005-3660	Linux kernel 2.4 and 2.6 allows attackers to cause a denial of service (memory exhaustion and panic) by creating a large number of socketpairs and setting a large data transfer buffer, then preventing Linux from being able to finish the transfer by closing the file descriptor without closing an associated reference.
CVE-2007-3719	The process scheduler in the Linux kernel 2.6.16 gives preference to "interactive" processes that perform voluntary context switches, as described in "Secretly Monopolizing the CPU Without Superuser Privileges".
CVE-2008-2544	Mounting /proc filesystem via chroot command silently mounts it in read-write mode. The user could bypass the chroot and modify files, he would never have otherwise.
CVE-2008-4609	The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco products allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipulate the connection queue, as demonstrated by sockstress.
CVE-2009-5155	In the GNU C Library (aka glibc or libc6) before 2.28, parse_reg_exp in posix/regcomp.c misparses alternatives, which can cause a denial of service (assertion failure and application exit) or trigger an incorrect result by attempting a regular-expression match.
CVE-2010-4563	The Linux kernel, when using IPv6, allows remote attackers to determine whether a host is sniffing the network by using a multicast address and determining whether an Echo Reply is sent, as demonstrated by thcping.
CVE-2010-5321	Memory leak in drivers/media/video/videobuf-core.c in the videobuf subsystem in the Linux kernel 2.6.x through 4.0.0 allows remote attackers to cause a denial of service (memory consumption) by leveraging /dev/video access for a series of mmap calls that require new allocations, as demonstrated by CVE-2007-6761. NOTE: as of 2016-06-18, this affects only 11 drivers that have not been updated to use videobuf2.
CVE-2011-4915	fs/proc/base.c in the Linux kernel through 3.1 allows local users to obtain sensitive keystroke information via access to /proc/kmsg.
CVE-2011-4916	Linux kernel through 3.1 allows local users to obtain sensitive keystroke information via access to /dev/pts/ and /dev/lp.
CVE-2011-4917	In the Linux kernel through 3.1 there is an information disclosure issue via /proc/stat.
CVE-2012-4542	block/scsi_ioctl.c in the Linux kernel through 3.8 does not properly consider the SCSI device class during authorization, which allows users to bypass intended access restrictions via an SG_IO ioctl call that leverages overlapping opcodes.
CVE-2012-6702	Expat, when used in a parser that has not called XML_SetHashSalt or passed it a seed of 0, makes it easier for attackers to bypass cryptographic protection mechanisms via vectors involving use of the srand function.
CVE-2012-6711	A heap-based buffer overflow exists in GNU Bash before 4.3 when wide characters, not supported by the current locale, are printed through the echo built-in function. A local attacker, who can provide data to print through the echo command, can cause a crash or execute code with the privileges of the bash process. This occurs because ansicstr() in lib/sh/strutils.c does not check for a null terminator.

CVE-2013-0341	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was w showed that it was not a security issue. Notes: none.
CVE-2013-1664	The XML libraries for Python 3.4, 3.3, 3.2, 3.1, 2.7, and 2.6, as used in OpenStack Keystone Essex, Folsom, and G Cinder Folsom; Django; and possibly other products allow remote attackers to cause a denial of service (resource c Expansion (XEE) attack.
CVE-2013-1665	The XML libraries for Python 3.4, 3.3, 3.2, 3.1, 2.7, and 2.6, as used in OpenStack Keystone Essex and Folsom, D remote attackers to read arbitrary files via an XML external entity declaration in conjunction with an entity referen attack.
CVE-2013-7040	<p>Python 2.7 before 3.4 only uses the last eight bits of the prefix to randomize hash values, which causes it to comput to trigger hash collisions predictably and makes it easier for context-dependent attackers to cause a denial of servic application that maintains a hash table.</p> <p> Note: This vulnerability exists because of an incomplete fix for CVE-2012-1150.</p>
CVE-2014-3477	The dbus-daemon in D-Bus 1.2.x through 1.4.x, 1.6.x before 1.6.20, and 1.8.x before 1.8.4, sends an AccessDenied the client is prohibited from accessing the service, which allows local users to cause a denial of service (initializatio channel attack via a D-Bus message to an inactive service.
CVE-2014-3532	dbus 1.3.0 before 1.6.22 and 1.8.x before 1.8.6, when running on Linux 2.6.37-rc4 or later, allows local users to cau of other services or applications) by sending a message containing a file descriptor, then exceeding the maximum r forwarded.
CVE-2014-3533	dbus 1.3.0 before 1.6.22 and 1.8.x before 1.8.6 allows local users to cause a denial of service (disconnect) via a cer the dbus-daemon to forward a message containing an invalid file descriptor.
CVE-2014-3564	Multiple heap-based buffer overflows in the status_handler function in (1) engine-gpgsm.c and (2) engine-uiscver attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to "different lin
CVE-2014-3566	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.
CVE-2014-3591	Libgcrypt before 1.6.3 and GnuPG before 1.4.19 does not implement ciphertext blinding for Elgamal decryption, w obtain the server's private key by determining factors using crafted ciphertext and the fluctuations in the electromag
CVE-2014-3636	D-Bus 1.3.0 through 1.6.x before 1.6.24 and 1.8.x before 1.8.8 allows local users to (1) cause a denial of service (p drop) by queuing the maximum number of file descriptors or (2) cause a denial of service (disconnect) via multiple allowed number of file descriptors for a single sendmsg call.
CVE-2014-3637	D-Bus 1.3.0 through 1.6.x before 1.6.24 and 1.8.x before 1.8.8 does not properly close connections for processes th to cause a denial of service via a D-bus message containing a D-Bus connection file descriptor.
CVE-2014-3638	The bus_connections_check_reply function in config-parser.c in D-Bus before 1.6.24 and 1.8.x before 1.8.8 allows consumption) via a large number of method calls.
CVE-2014-3639	The dbus-daemon in D-Bus before 1.6.24 and 1.8.x before 1.8.8 does not properly close old connections, which all (incomplete connection consumption and prevention of new connections) via a large number of incomplete connec
CVE-2014-4043	The posix_spawn_file_actions_addopen function in glibc before 2.20 does not copy its path argument in accordance context-dependent attackers to trigger use-after-free vulnerabilities.
CVE-2014-4617	The do_uncompress function in g10/compress.c in GnuPG 1.x before 1.4.17 and 2.x before 2.0.24 allows context-c service (infinite loop) via malformed compressed packets, as demonstrated by an a3 01 5b ff byte sequence.
CVE-2014-5044	Multiple integer overflows in libgfortran might allow remote attackers to execute arbitrary code or cause a denial o vectors related to array allocation.
CVE-2014-5270	Libgcrypt before 1.5.4, as used in GnuPG and other products, does not properly perform ciphertext normalization a easier for physically proximate attackers to conduct key-extraction attacks by leveraging the ability to collect volta than CVE-2013-4576.
CVE-2014-5351	The kadm5_randkey_principal_3 function in lib/kadm5/srv/svr_principal.c in kadmind in MIT Kerberos 5 (aka krb a -randkey -keepold request, which allows remote authenticated users to forge tickets by leveraging administrative
CVE-2014-5461	Buffer overflow in the vararg functions in ldo.c in Lua 5.1 through 5.2.x before 5.2.3 allows context-dependent atta a small number of arguments to a function with a large number of fixed arguments.
CVE-2014-9114	Blkid in util-linux before 2.26rc-1 allows local users to execute arbitrary code.
CVE-2014-9620	The ELF parser in file 5.08 through 5.21 allows remote attackers to cause a denial of service via a large number of

CVE-2014-9892	The <code>snd_compr_tstamp</code> function in <code>sound/core/compress_offload.c</code> in the Linux kernel through 4.7, as used in Android (2013) devices, does not properly initialize a timestamp data structure, which allows attackers to obtain sensitive information via a crafted application. Android internal bug 28770164 and Qualcomm internal bug CR568717.
CVE-2014-9900	The <code>ethtool_get_wol</code> function in <code>net/core/ethtool.c</code> in the Linux kernel through 4.7, as used in Android before 2016, does not initialize a certain data structure, which allows local users to obtain sensitive information via a crafted application. Qualcomm internal bug CR570754.
CVE-2014-9939	<code>ihex.c</code> in GNU Binutils before 2.26 contains a stack buffer overflow when printing bad bytes in Intel Hex objects.
CVE-2015-0245	D-Bus 1.4.x through 1.6.x before 1.6.30, 1.8.x before 1.8.16, and 1.9.x before 1.9.10 does not validate the source of a message, which allows local users to cause a denial of service (activation failure error returned) by leveraging a race condition involving <code>systemd</code> responds.
CVE-2015-0247	Heap-based buffer overflow in <code>openfs.c</code> in the <code>libext2fs</code> library in <code>e2fsprogs</code> before 1.42.12 allows local users to extract sensitive descriptor data in a filesystem image.
CVE-2015-0837	The <code>mpi_powm</code> function in <code>Libgcrypt</code> before 1.6.3 and <code>GnuPG</code> before 1.4.19 allows attackers to obtain sensitive information when accessing a pre-computed table during modular exponentiation, related to a "Last-Level Cache Side-Channel" attack.
CVE-2015-1197	<code>cpio</code> 2.11, when using the <code>--no-absolute-filenames</code> option, allows local users to write to arbitrary files via a symlink.
CVE-2015-1572	Heap-based buffer overflow in <code>closefs.c</code> in the <code>libext2fs</code> library in <code>e2fsprogs</code> before 1.42.12 allows local users to extract sensitive block group descriptor to be marked as dirty. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-0247.
CVE-2015-1606	The keyring DB in <code>GnuPG</code> before 2.1.2 does not properly handle invalid packets, which allows remote attackers to cause a denial of service (use-after-free) via a crafted keyring file.
CVE-2015-1607	<code>kbx/keybox-search.c</code> in <code>GnuPG</code> before 1.4.19, 2.0.x before 2.0.27, and 2.1.x before 2.1.2 does not properly handle invalid packets, which allows attackers to cause a denial of service (invalid read operation) via a crafted keyring file, related to sign extensions and keybox search.
CVE-2015-2059	The <code>stringprep_utf8_to_ucs4</code> function in <code>libin</code> before 1.31, as used in <code>jabberd2</code> , allows context-dependent attackers to cause a denial of service (other unspecified impact via invalid UTF-8 characters in a string, which triggers an out-of-bounds read).
CVE-2015-2327	PCRE before 8.36 mishandles the <code>/((a2)(a*)g<-1>)*</code> pattern and related patterns with certain internal recursive calls, which allows attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by JavaScript RegExp object encountered by Konqueror.
CVE-2015-2328	PCRE before 8.36 mishandles the <code>/((?R)a(?!))+/</code> pattern and related patterns with certain recursion, which allows attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by Konqueror.
CVE-2015-2613	Unspecified vulnerability in Oracle Java SE 7u80 and 8u45, and Java SE Embedded 7u75 and 8u33 allows remote attackers to cause a denial of service (related to JCE).
CVE-2015-2695	<code>lib/gssapi/spnego/spnego_mech.c</code> in MIT Kerberos 5 (aka <code>krb5</code>) before 1.14 relies on an inappropriate context handle, which allows remote attackers to cause a denial of service (incorrect pointer read and process crash) via a crafted SPNEGO packet that is mishandled during a GSSAPI exchange.
CVE-2015-2696	<code>lib/gssapi/krb5/iakerb.c</code> in MIT Kerberos 5 (aka <code>krb5</code>) before 1.14 relies on an inappropriate context handle, which allows remote attackers to cause a denial of service (incorrect pointer read and process crash) via a crafted IAKERB packet that is mishandled during a GSSAPI exchange.
CVE-2015-2697	The <code>build_principal_va</code> function in <code>lib/krb5/krb/bld_princ.c</code> in MIT Kerberos 5 (aka <code>krb5</code>) before 1.14 allows remote attackers to cause a denial of service (out-of-bounds read and KDC crash) via an initial '\0' character in a long realm field within a TGS request.
CVE-2015-2808	The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key schedule, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "RC4 Invariance Weakness".
CVE-2015-2877	Kernel Samepage Merging (KSM) in the Linux kernel 2.6.32 through 4.x does not prevent use of a write-timing side channel to defeat the ASLR protection mechanism on other guest OS instances via a Cross-VM ASLR INTrospection (CAIN) attack. If you care about this attack vector, disable deduplication. Share-until-written approaches for memory conservation are inherently detectable for information disclosure, and can be classified as potentially misunderstood behaviors rather than bugs.
CVE-2015-3153	The default configuration for <code>cURL</code> and <code>libcurl</code> before 7.42.1 sends custom HTTP headers to both the proxy and destination servers to obtain sensitive information by reading the header contents.
CVE-2015-3217	PCRE 7.8 and 8.32 through 8.37, and PCRE2 10.10 mishandle group empty matches, which might allow remote attackers to cause a denial of service (based buffer overflow) via a crafted regular expression, as demonstrated by <code>/^((?:1) \ ([^\ \\W_])?)++)\$</code> .
CVE-2015-5073	Heap-based buffer overflow in the <code>find_fixedlength</code> function in <code>pcrc_compile.c</code> in PCRE before 8.38 allows remote attackers to obtain sensitive information from heap memory and possibly bypass the ASLR protection mechanism via a crafted regular expression.
CVE-2015-5186	<code>Audit</code> before 2.4.4 in Linux does not sanitize escape characters in filenames.

CVE-2015-5218	Buffer overflow in text-utils/colcrt.c in colcrt in util-linux before 2.27 allows local users to cause a denial of service via a crafted global variable.
CVE-2015-5276	The std::random_device class in libstdc++ in the GNU Compiler Collection (aka GCC) before 4.9.4 does not properly seed random values, which makes it easier for context-dependent attackers to predict the random values via unspecified vectors.
CVE-2015-7036	The fits3_tokenizer function in SQLite, as used in Apple iOS before 8.4 and OS X before 10.10.4, allows remote attackers to cause a denial of service (application crash) via a SQL command that triggers an API call with a crafted pointer value in the statement object.
CVE-2015-8382	The match function in pcre_exec.c in PCRE before 8.37 mishandles the /(?:((abcd))(((?:(?:?:abc(?:abcdef))))b))) pattern and related patterns involving (*ACCEPT), which allows remote attackers to obtain sensitive information from process memory (partially initialized memory and application crash) via a crafted regular expression, as demonstrated by a JavaScripT aka ZDI-CAN-2547.
CVE-2015-8386	PCRE before 8.38 mishandles the interaction of lookbehind assertions and mutually recursive subpatterns, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by Konqueror.
CVE-2015-8388	PCRE before 8.38 mishandles the /(?=di(?<=?1))(?=(.)))/ pattern and related patterns with an unmatched closing parenthesis, which causes a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression executed by an object encountered by Konqueror.
CVE-2015-8391	The pcre_compile function in pcre_compile.c in PCRE before 8.38 mishandles certain [[: nesting, which allows remote attackers to cause a denial of service (CPU consumption) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by Konqueror.
CVE-2015-8538	dwarf_leb.c in libdwf allows attackers to cause a denial of service (SIGSEGV).
CVE-2015-8865	The file_check_mem function in funcs.c in file before 5.23, as used in the Fileinfo component in PHP before 5.5.34, mishandles continuation-level jumps, which allows context-dependent attackers to cause a denial of service (buffer overflow) and execute arbitrary code via a crafted magic file.
CVE-2015-8948	idn in GNU libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero-length bounds read.
CVE-2015-8982	Integer overflow in the strxfrm function in the GNU C Library (aka glibc or libc6) before 2.21 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.
CVE-2015-8982	Integer overflow in the strxfrm function in the GNU C Library (aka glibc or libc6) before 2.21 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.
CVE-2015-8983	Integer overflow in the _IO_wstr_overflow function in libio/wstrops.c in the GNU C Library (aka glibc or libc6) before 2.21 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to computing a string length, which triggers a buffer overflow.
CVE-2015-8983	Integer overflow in the _IO_wstr_overflow function in libio/wstrops.c in the GNU C Library (aka glibc or libc6) before 2.21 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to computing a string length, which triggers a buffer overflow.
CVE-2015-8984	The fnmatch function in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attackers to cause a denial of service (crash) via a malformed pattern, which triggers an out-of-bounds read.
CVE-2015-8985	The pop_fail_stack function in the GNU C Library (aka glibc or libc6) allows context-dependent attackers to cause a denial of service (application crash) via vectors related to extended regular expression processing.
CVE-2016-0755	The ConnectionExists function in lib/url.c in libcurl before 7.47.0 does not properly re-use NTLM-authenticated proxy connections, which allows attackers to authenticate as other users via a request, a similar issue to CVE-2014-0015.
CVE-2016-10228	The iconv program in the GNU C Library (aka glibc or libc6) 2.31 and earlier, when invoked with multiple suffixes (-s or IGNORE) along with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.
CVE-2016-10254	The allocate_elf function in common.h in elfutils before 0.168 allows remote attackers to cause a denial of service (memory allocation failure).
CVE-2016-10255	The __libelf_set_rawdata_wrlock function in elf_getdata.c in elfutils before 0.168 allows remote attackers to cause a denial of service (sh_offset or (2) sh_size ELF header value, which triggers a memory allocation failure).
CVE-2016-10255	The __libelf_set_rawdata_wrlock function in elf_getdata.c in elfutils before 0.168 allows remote attackers to cause a denial of service (sh_offset or (2) sh_size ELF header value, which triggers a memory allocation failure).
CVE-2016-10255	The __libelf_set_rawdata_wrlock function in elf_getdata.c in elfutils before 0.168 allows remote attackers to cause a denial of service (sh_offset or (2) sh_size ELF header value, which triggers a memory allocation failure).
CVE-2016-10505	NULL pointer dereference vulnerabilities in the imagetopnm function in convert.c, sycc444_to_rgb function in color.c, and sycc422_to_rgb function in color.c in OpenJPEG before 2.2.0 allow remote attackers to cause a denial of service via crafted input.

CVE-2016-10506	Division-by-zero vulnerabilities in the functions <code>opj_pi_next_cpri</code> , <code>opj_pi_next_pcri</code> , and <code>opj_pi_next_rpci</code> in <code>pi.c</code> in <code>libjpeg-turbo</code> allow remote attackers to cause a denial of service (application crash) via crafted j2k files.
CVE-2016-10723	An issue was discovered in the Linux kernel through 4.17.2. Since the page allocator does not yield CPU resources to a non-privileged user can trivially lock up the system forever by wasting CPU resources from the page allocator (e.g., by allocating a large number of pages). A global OOM killer is invoked. NOTE: the software maintainer has not accepted certain proposed patches, in part because the problem is non-trivial to handle.
CVE-2016-1234	Stack-based buffer overflow in the <code>glob</code> implementation in GNU C Library (aka glibc) before 2.24, when <code>GLOB_APPEND</code> is used, allows remote attackers to cause a denial of service (crash) via a long name.
CVE-2016-1938	The <code>s_mp_div</code> function in <code>lib/freebl/mpi/mpi.c</code> in Mozilla Network Security Services (NSS) before 3.21, as used in Firefox, divides numbers, which might make it easier for remote attackers to defeat cryptographic protection mechanisms by using the <code>mp_exptmod</code> function.
CVE-2016-1951	Multiple integer overflows in <code>io/prprf.c</code> in Mozilla Netscape Portable Runtime (NSPR) before 4.12 allow remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a long string to a <code>PR_*printf</code> function.
CVE-2016-2037	The <code>cpio_safer_name_suffix</code> function in <code>util.c</code> in <code>cpio</code> 2.11 allows remote attackers to cause a denial of service (out of memory) via a long filename.
CVE-2016-2183	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPsec protocols and other protocols and products, allow remote attackers to obtain cleartext data via a birthday attack against a long session key, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.
CVE-2016-2226	Integer overflow in the <code>string_appends</code> function in <code>cplus-dem.c</code> in <code>libiberty</code> allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow) via a long string.
CVE-2016-2779	<code>runuser</code> in <code>util-linux</code> allows local users to escape to the parent session via a crafted <code>TIOCSTI</code> ioctl call, which pushes the user to the parent session.
CVE-2016-3189	Use-after-free vulnerability in <code>bzip2recover</code> in <code>bzip2</code> 1.0.6 allows remote attackers to cause a denial of service (crash) via a file whose ends set to before the start of the block.
CVE-2016-4008	The <code>_asn1_extract_der_octet</code> function in <code>lib/decoding.c</code> in GNU Libtasn1 before 4.8, when used without the <code>ASN1_CHECKED_COPY</code> flag, allows remote attackers to cause a denial of service (infinite recursion) via a crafted certificate.
CVE-2016-4429	Stack-based buffer overflow in the <code>clntudp_call</code> function in <code>sunrpc/clnt_udp.c</code> in the GNU C Library (aka glibc or libc) allows remote attackers to cause a denial of service (crash) or possibly unspecified other impact via a flood of crafted ICMP and UDP packets.
CVE-2016-4472	The overflow protection in Expat is removed by compilers with certain optimization settings, which allows remote attackers to cause a denial of service (out of memory) or possibly execute arbitrary code via crafted XML data. NOTE: this vulnerability exists because of an incomplete fix.
CVE-2016-4483	The <code>xmlBufAttrSerializeTxtContent</code> function in <code>xmlsave.c</code> in <code>libxml2</code> allows context-dependent attackers to cause a denial of service (application crash) via a non-UTF-8 attribute value, related to serialization. NOTE: this vulnerability may be a duplicate of CVE-2016-4484.
CVE-2016-4484	The Debian <code>initrd</code> script for the <code>cryptsetup</code> package 2:1.7.3-2 and earlier allows physically proximate attackers to guess the root password via an invalid password.
CVE-2016-4487	Use-after-free vulnerability in <code>libiberty</code> allows remote attackers to cause a denial of service (segmentation fault and crash) via a "btypevec."
CVE-2016-4488	Use-after-free vulnerability in <code>libiberty</code> allows remote attackers to cause a denial of service (segmentation fault and crash) via a "ktypevec."
CVE-2016-4489	Integer overflow in the <code>gnu_special</code> function in <code>libiberty</code> allows remote attackers to cause a denial of service (segmentation fault and crash) related to the "demangling of virtual tables."
CVE-2016-4490	Integer overflow in <code>cp-demangle.c</code> in <code>libiberty</code> allows remote attackers to cause a denial of service (segmentation fault and crash) via inconsistent use of the long and int types for lengths.
CVE-2016-4491	The <code>d_print_comp</code> function in <code>cp-demangle.c</code> in <code>libiberty</code> allows remote attackers to cause a denial of service (segmentation fault and crash) which triggers infinite recursion and a buffer overflow, related to a node having "itself as ancestor more than once."
CVE-2016-4492	Buffer overflow in the <code>do_type</code> function in <code>cplus-dem.c</code> in <code>libiberty</code> allows remote attackers to cause a denial of service (crash) via a crafted binary.
CVE-2016-4493	The <code>demangle_template_value_parm</code> and <code>do_hpace_template_literal</code> functions in <code>cplus-dem.c</code> in <code>libiberty</code> allow remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted binary.
CVE-2016-4984	<code>/usr/libexec/openssl/generate-server-cert.sh</code> in <code>openssl-servers</code> sets weak permissions for the TLS certificate, which can be leveraged by a race condition between the creation of the certificate, and the <code>chmod</code> to protect it.
CVE-2016-5300	The XML parser in Expat does not use sufficient entropy for hash initialization, which allows context-dependent attackers to cause a denial of service (consumption of memory) via crafted identifiers in an XML document. NOTE: this vulnerability exists because of an incomplete fix.

CVE-2016-6153	os_unix.c in SQLite before 3.13.0 improperly implements the temporary directory search algorithm, which might allow an attacker to cause a denial of service (application crash), or have unspecified other impact by leveraging use of the files.
CVE-2016-6261	The idna_to_ascii_4i function in lib/idna.c in libidn before 1.33 allows context-dependent attackers to cause a denial of service (application crash) via 64 bytes of input.
CVE-2016-6262	idn in libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte via read, a different vulnerability than CVE-2015-8948.
CVE-2016-6263	The stringprep_utf8_nfkc_normalize function in lib/nfkc.c in libidn before 1.33 allows context-dependent attackers to cause a denial of service (application crash) via crafted UTF-8 data.
CVE-2016-6318	Stack-based buffer overflow in the FascistGecosUser function in lib/fascist.c in cracklib allows local users to cause a denial of service (application crash) and possibly obtain sensitive information via a long GECOS field, involving longbuffer.
CVE-2016-6321	Directory traversal vulnerability in the safer_name_suffix function in GNU tar 1.14 through 1.29 might allow remote attackers to read arbitrary files via the --dereference option and write to arbitrary files via vectors related to improper sanitization of the file_name parameter, aka "tar --dereference --file-name-sanitization" (CVE-2016-6321).
CVE-2016-6349	The machinectl command in oci-register-machine allows local users to list running containers and possibly obtain sensitive information via the --show command.
CVE-2016-7091	sudo: It was discovered that the default sudo configuration on Red Hat Enterprise Linux and possibly other Linux distributions allows a local user to bypass the INPUTRC which could lead to information disclosure. A local user with sudo access to a restricted program that uses the sudoers file can read from specially formatted files with elevated privileges provided by sudo.
CVE-2016-8615	A flaw was found in curl before version 7.51. If cookie state is written into a cookie jar file that is later read back at a later time, an HTTP server can inject new cookies for arbitrary domains into said cookie jar.
CVE-2016-8616	A flaw was found in curl before version 7.51.0 When re-using a connection, curl was doing case insensitive comparison of hostnames for existing connections. This means that if an unused connection with proper credentials exists for a protocol that has a case sensitive password, it can cause that connection to be reused if s/he knows the case-insensitive version of the correct password.
CVE-2016-8617	The base64 encode function in curl before version 7.51.0 is prone to a buffer being under allocated in 32bit systems due to the use of the `CURLOPT_USERNAME`.
CVE-2016-8618	The libcurl API function called `curl_maprintf()` before version 7.51.0 can be tricked into doing a double-free due to the use of the `size_t` variables.
CVE-2016-8619	The function `read_data()` in security.c in curl before version 7.51.0 is vulnerable to memory double free.
CVE-2016-8621	The `curl_getdate` function in curl before version 7.51.0 is vulnerable to an out of bounds read if it receives an input that is not a valid date.
CVE-2016-8622	The URL percent-encoding decode function in libcurl before 7.51.0 is called `curl_easy_unescape`. Internally, even if the unescape destination buffer is larger than 2GB, it would return that new length in a signed 32 bit integer variable, thus causing the length to be both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer.
CVE-2016-8623	A flaw was found in curl before version 7.51.0. The way curl handles cookies permits other threads to trigger a use after free.
CVE-2016-8624	curl before version 7.51.0 doesn't parse the authority component of the URL correctly when the host name part ends with a dot. This may have security implications if you for example use an URL parser that parses domains before using curl to request them.
CVE-2016-8625	curl before version 7.51.0 uses outdated IDNA 2003 standard to handle International Domain Names and this may cause network transfer requests to the wrong host.
CVE-2016-9063	An integer overflow during the parsing of XML using the Expat library. This vulnerability affects Firefox < 50.
CVE-2016-9074	An existing mitigation of timing side-channel attacks is insufficient in some circumstances. This issue is addressed in Firefox 50. This vulnerability affects Thunderbird < 45.5, Firefox ESR < 45.5, and Firefox < 50.
CVE-2016-9113	There is a NULL pointer dereference in function imagetobmp of convertbmp.c:980 of OpenJPEG 2.1.2. image->convertbmp initialization(NULL). Impact is Denial of Service.
CVE-2016-9114	There is a NULL Pointer Access in function imagetopnm of convert.c:1943(jp2) of OpenJPEG 2.1.2. image->converttopnm initialization(NULL). Impact is Denial of Service.
CVE-2016-9115	Heap Buffer Over-read in function imagetotga of convert.c(jp2):942 in OpenJPEG 2.1.2. Impact is Denial of Service.
CVE-2016-9116	NULL Pointer Access in function imagetopnm of convert.c:2226(jp2) in OpenJPEG 2.1.2. Impact is Denial of Service.
CVE-2016-9117	NULL Pointer Access in function imagetopnm of convert.c(jp2):1289 in OpenJPEG 2.1.2. Impact is Denial of Service.
CVE-2016-9318	libxml2 2.9.4 and earlier, as used in XMLSec 1.2.23 and earlier and other products, does not offer a flag directly in the read but other files may not be opened, which makes it easier for remote attackers to conduct XML External Entity (XXE) attacks.
CVE-2016-9574	nss before version 3.30 is vulnerable to a remote denial of service during the session handshake when using Session ID.

CVE-2016-9580	An integer overflow vulnerability was found in tftoimage function in openjpeg 2.1.2, resulting in heap buffer over
CVE-2016-9581	An infinite loop vulnerability in tftoimage that results in heap buffer overflow in convert_32s_C1P1 was found in
CVE-2016-9586	curl before version 7.52.0 is vulnerable to a buffer overflow when doing a large floating point output in libcurl's im are any application that accepts a format string from the outside without necessary input filtering, it could allow rem
CVE-2017-0630	An information disclosure vulnerability in the kernel trace subsystem could enable a local malicious application to This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Vers A-34277115.
CVE-2017-0663	A remote code execution vulnerability in libxml2 could enable an attacker using a specially crafted file to execute a unprivileged process. This issue is rated as High due to the possibility of remote code execution in an application th Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37104170.
CVE-2017-1000100	When doing a TFTP transfer and curl/libcurl is given a URL that contains a very long file name (longer than about within the buffer boundaries, but the buffer size is still wrongly updated to use the untruncated length. This too larg making curl attempt to send more data than what is actually put into the buffer. The endto() function will then read A malicious HTTP(S) server could redirect a vulnerable libcurl-using client to a crafted TFTP URL (if the client ha redirects to) and trick it to send private memory contents to a remote server over UDP. Limit curl's redirect protoco CURLOPT_REDIR_PROTOCOLS.
CVE-2017-1000158	CPython (aka Python) up to 2.7.13 is vulnerable to an integer overflow in the PyString_DecodeEscape function in overflow (and possible arbitrary code execution)
CVE-2017-1000254	libcurl may read outside of a heap allocated buffer when doing FTP. When libcurl connects to an FTP server and su asks the server for the current directory with the `PWD` command. The server then responds with a 257 response c The returned path name is then kept by libcurl for subsequent uses. Due to a flaw in the string parser for this direct but without a closing double quote would lead to libcurl not adding a trailing NUL byte to the buffer holding the na the string, it could read beyond the allocated heap buffer and crash or wrongly access data beyond the buffer, think server could abuse this fact and effectively prevent libcurl-based clients to work with it - the PWD command is alw mistake has a high chance of causing a segfault. The simple fact that this has issue remained undiscovered for this responses are rare in benign servers. We are not aware of any exploit of this flaw. This bug was introduced in comm commit/415d2e7cb7), March 2005. In libcurl version 7.56.0, the parser always zero terminates the string but also r double quote.
CVE-2017-10140	Postfix before 2.11.10, 3.0.x before 3.0.10, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 might allow local users to gain functionality in Berkeley DB 2.x and later, related to reading settings from DB_CONFIG in the current directory.
CVE-2017-10684	In ncurses 6.0, there is a stack-based buffer overflow in the fmt_entry function. A crafted input will lead to a remot
CVE-2017-10685	In ncurses 6.0, there is a format string vulnerability in the fmt_entry function. A crafted input will lead to a remote
CVE-2017-10790	The _asn1_check_identifier function in GNU Libtasn1 through 4.12 causes a NULL pointer dereference and crash assignment of a NULL value within an asn1_node structure. It may lead to a remote denial of service attack.
CVE-2017-10989	The getNodeSize function in ext/rtree/rtree.c in SQLite through 3.19.3, as used in GDAL and other products, mish database, leading to a heap-based buffer over-read or possibly unspecified other impact.
CVE-2017-11112	In ncurses 6.0, there is an attempted 0xffffffffffff access in the append_acs function of tinfo/parse_entry.c. It co the terminfo library code is used to process untrusted terminfo data.
CVE-2017-11113	In ncurses 6.0, there is a NULL Pointer Dereference in the _nc_parse_entry function of tinfo/parse_entry.c. It coul the terminfo library code is used to process untrusted terminfo data.
CVE-2017-11462	Double free vulnerability in MIT Kerberos 5 (aka krb5) allows attackers to have unspecified impact via vectors inv on error.
CVE-2017-12449	The _bfd_vms_save_sized_string function in vms-misc.c in the Binary File Descriptor (BFD) library (aka libbfd), earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms file.
CVE-2017-12451	The _bfd_xcoff_read_ar_hdr function in bfd/coff-rs6000.c and bfd/coff64-rs6000.c in the Binary File Descriptor (B GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds stack read via a crafted COFF im
CVE-2017-12452	The bfd_mach_o_i386_canonicalize_one_reloc function in bfd/mach-o-i386.c in the Binary File Descriptor (BFD) Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted mach-o file.
CVE-2017-12453	The _bfd_vms_slurp_eom function in libbfd.c in the Binary File Descriptor (BFD) library (aka libbfd), as distribu remote attackers to cause an out of bounds heap read via a crafted vms alpha file.
CVE-2017-12454	The _bfd_vms_slurp_egsd function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as allows remote attackers to cause an arbitrary memory read via a crafted vms alpha file.
CVE-2017-12455	The evax_bfd_print_emh function in vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distri allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.

CVE-2017-12456	The read_symbol_stabs_debugging_info function in rddbg.c in GNU Binutils 2.29 and earlier allows remote attackers to cause a denial of service (stack-based buffer over-read and application crash) via a crafted binary file.
CVE-2017-12457	The bfd_make_section_with_flags function in section.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a NULL dereference via a crafted file.
CVE-2017-12458	The nlm_swap_auxiliary_headers_in function in bfd/nlmcodes.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted nlm file.
CVE-2017-12799	The elf_read_notes function in bfd/elf.c in GNU Binutils 2.29 allows remote attackers to cause a denial of service (denial of service) via a crafted binary file.
CVE-2017-12967	The getsym function in tekhex.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (stack-based buffer over-read and application crash) via a malformed tekhex binary.
CVE-2017-13685	The dump_callback function in SQLite 3.20.0 allows remote attackers to cause a denial of service (EXC_BAD_ACCESS) via a crafted binary file.
CVE-2017-13694	The acpi_ps_complete_final_op() function in drivers/acpi/acpica/psobject.c in the Linux kernel through 4.12.9 does not validate the length of the ACPI table, which causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass security restrictions (kernel through 4.9) via a crafted ACPI table.
CVE-2017-13710	The setup_group function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a group section that is too small.
CVE-2017-13728	There is an infinite loop in the next_char function in comp_scan.c in ncurses 6.0, related to libtinfo. A crafted input will cause a denial of service (infinite loop) via a crafted input.
CVE-2017-13729	There is an illegal address access in the _nc_save_str function in alloc_entry.c in ncurses 6.0. It will lead to a remote denial of service (infinite loop) via a crafted input.
CVE-2017-13730	There is an illegal address access in the function _nc_read_entry_source() in progs/tic.c in ncurses 6.0 that might lead to a remote denial of service (infinite loop) via a crafted input.
CVE-2017-13731	There is an illegal address access in the function postprocess_termcap() in parse_entry.c in ncurses 6.0 that will lead to a remote denial of service (infinite loop) via a crafted input.
CVE-2017-13732	There is an illegal address access in the function dump_uses() in progs/dump_entry.c in ncurses 6.0 that might lead to a remote denial of service (infinite loop) via a crafted input.
CVE-2017-13733	There is an illegal address access in the fmt_entry function in progs/dump_entry.c in ncurses 6.0 that might lead to a remote denial of service (infinite loop) via a crafted input.
CVE-2017-13734	There is an illegal address access in the _nc_safe_strerror function in strings.c in ncurses 6.0 that will lead to a remote denial of service (infinite loop) via a crafted input.
CVE-2017-13757	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not validate the PLT entry for a symbol, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to elf32-i386.c and elf_x86_64_get_synthetic_symtab in elf64-x86-64.c.
CVE-2017-14062	Integer overflow in the decode_digit function in puny_decode.c in Libidn2 before 2.0.4 allows remote attackers to cause a denial of service (integer overflow and application crash) via a crafted input.
CVE-2017-14128	The decode_line_info function in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (read_1_byte heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-14129	The read_section function in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (parse_comp_unit heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-14130	The _bfd_elf_parse_attributes function in elf-attrs.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (_bfd_elf_attr_strdup heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-14529	The pe_print_pdata function in peXXigen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-14729	The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c.
CVE-2017-14745	The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allow remote attackers to cause a denial of service (integer overflow and application crash) via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c.
CVE-2017-14930	Memory leak in decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file.
CVE-2017-14932	decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite loop) via a crafted ELF file.
CVE-2017-14933	read_formatted_entries in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite loop) via a crafted ELF file.


CVE-2017-14934	process_debug_info in dwarf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite loop) via a crafted ELF file that contains a negative size value in a CU structure.
CVE-2017-14938	_bfd_elf_slurp_version_tables in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted ELF file.
CVE-2017-14939	decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-14940	scan_unit_for_symbols in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file.
CVE-2017-14974	The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c.
CVE-2017-15020	dwarf1.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file, related to parse_die heap-based buffer over-read.
CVE-2017-15021	bfd_get_debug_link_info_1 in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to bfd_get_debug_link_info_1.
CVE-2017-15022	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not validate remote attackers to cause a denial of service (bfd_hash_hash NULL pointer dereference, or out-of-bounds access and application crash) via a crafted ELF file, related to scan_unit_for_symbols and parse_comp_unit.
CVE-2017-15023	read_formatted_entries in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file, related to concat_filename.
CVE-2017-15024	find_abstract_instance_name in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite recursion and application crash) via a crafted ELF file.
CVE-2017-15025	decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted ELF file.
CVE-2017-15088	plugins/preauth/pkinit/pkinit_crypto_openssl.c in MIT Kerberos 5 (aka krb5) through 1.15.2 mishandles Distinguished Name (DN) data and allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) in situations involving the use of get_matching_data and X509_NAME_oneline_ex functions. NOTE: this has security relevance only in use cases of the use of get_matching_data in KDC certauth plugin code that is specific to Red Hat.
CVE-2017-15225	_bfd_dwarf2_cleanup_debug_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (memory leak) via a crafted ELF file.
CVE-2017-15286	SQLite 3.20.1 has a NULL pointer dereference in tableColumnList in shell.c because it fails to consider certain cases where `sqlite3_step(pStmt)==SQLITE_ROW` is false and a data structure is never initialized.
CVE-2017-15671	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27, when invoked with GLOB_TILDE, allows remote attackers to cause a denial of service (memory leak) when processing the ~ operator with a long user name, potentially leading to a denial of service (memory leak).
CVE-2017-15938	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, miscalculates the size of a relocatable object file, which allows remote attackers to cause a denial of service (find_abstract_instance_name NULL pointer dereference and application crash).
CVE-2017-15939	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file.  Note: This issue is caused by an incomplete fix for CVE-2017-15023.
CVE-2017-15996	elfcomm.c in readelf in GNU Binutils 2.29 allows remote attackers to cause a denial of service (excessive memory impact) via a crafted ELF file that triggers a "buffer overflow on fuzzed archive header," related to an uninitialized buffer in the get_archive_member_name, process_archive_index_and_symbols, and setup_archive functions.
CVE-2017-16826	The coff_slurp_line_table function in coffcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (invalid memory access and application crash) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-16827	The aout_get_external_symbols function in aoutx.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (slurp_symtab invalid free and application crash) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-16828	The display_debug_frames function in dwarf.c in GNU Binutils 2.29.1 allows remote attackers to cause a denial of service (buffer over-read, and application crash) or possibly have unspecified other impact via a crafted ELF file, related to display_debug_frames.

CVE-2017-16829	The <code>_bfd_elf_parse_gnu_properties</code> function in <code>elf-properties.c</code> in the Binary File Descriptor (BFD) library (aka libbfd) does not prevent negative pointers, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-16830	The <code>print_gnu_property_note</code> function in <code>readelf.c</code> in GNU Binutils 2.29.1 does not have integer-overflow protection, which allows remote attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-16831	<code>coffgen.c</code> in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not validate the size of the external string table, which allows remote attackers to cause a denial of service (integer overflow and application crash, or excessive memory allocation) or possibly have unspecified other impact via a crafted PE file.
CVE-2017-16832	The <code>pe_bfd_read_buildid</code> function in <code>peicode.h</code> in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not validate the size and offset values in the data dictionary, which allows remote attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact via a crafted PE file.
CVE-2017-16879	Stack-based buffer overflow in the <code>_nc_write_entry</code> function in <code>tinio/write_entry.c</code> in ncurses 6.0 allows attackers to cause a denial of service (segmentation violation and application crash) or possibly execute arbitrary code via a crafted terminfo file, as demonstrated by tic.
CVE-2017-16931	<code>parser.c</code> in libxml2 before 2.9.5 mishandles parameter-entity references because the NEXTL macro calls the <code>xmlParseEntity</code> function with a '%' character in a DTD name.
CVE-2017-16932	<code>parser.c</code> in libxml2 before 2.9.5 does not prevent infinite recursion in parameter entities.
CVE-2017-17080	<code>elf.c</code> in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not validate the size of the external string table, which allows remote attackers to cause a denial of service (bfd_get32 heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-17121	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, allows remote attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact via a COFF binary in which a relocation refers to a local symbol.
CVE-2017-17122	The <code>dump_relocs_in_section</code> function in <code>objdump.c</code> in GNU Binutils 2.29.1 does not check for reloc count integer overflow, which allows remote attackers to cause a denial of service (excessive memory allocation, or heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted PE file.
CVE-2017-17123	The <code>coff_slurp_reloc_table</code> function in <code>coffcode.h</code> in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not validate the size of the external string table, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted COFF based file.
CVE-2017-17124	The <code>_bfd_coff_read_string_table</code> function in <code>coffgen.c</code> in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not properly validate the size of the external string table, which allows remote attackers to cause a denial of service (excessive memory allocation, or heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted COFF binary.
CVE-2017-17125	<code>nm.c</code> and <code>objdump.c</code> in GNU Binutils 2.29.1 mishandle certain global symbols, which allows remote attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-17126	The <code>load_debug_section</code> function in <code>readelf.c</code> in GNU Binutils 2.29.1 allows remote attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact via an ELF file that lacks section headers.
CVE-2017-17479	In OpenJPEG 2.3.0, a stack-based buffer overflow was discovered in the <code>pgxtoimage</code> function in <code>jpwl/convert.c</code> . The overflow occurs when processing a crafted input file, which may lead to remote denial of service or possibly remote code execution.
CVE-2017-18078	systemd-tmpfiles in systemd before 237 attempts to support ownership/permission changes on hardlinked files even when the <code>ForceDelete</code> option is turned off, which allows local users to bypass intended access restrictions via vectors involving a hard link to a file. A proof of concept exploit is demonstrated by changing the ownership of the <code>/etc/passwd</code> file.
CVE-2017-18640	The Alias feature in SnakeYAML before 1.26 allows entity expansion during a load operation, a related issue to CVE-2017-18641.
CVE-2017-5969	libxml2 2.9.4, when used in recover mode, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via a crafted XML file. NOTE: The maintainer states "I would disagree of a CVE with the Recover parsing option which should only be used for debugging".
CVE-2017-6004	The <code>compile_bracket_matchingpath</code> function in <code>pcr_jit_compile.c</code> in PCRE through 8.x before revision 1680 (e.g., 8.36) allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted regular expression.
CVE-2017-6891	Two errors in the <code>"asn1_find_node()"</code> function (<code>lib/parser_aux.c</code>) within GnuTLS libtasn1 version 4.10 can be exploited to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact by tricking a user into processing a specially crafted assignments file via the e.g. <code>asn1Coding</code> utility.
CVE-2017-6965	<code>readelf</code> in GNU Binutils 2.28 writes to illegal addresses while processing corrupt input files containing symbol-diff information, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-6966	<code>readelf</code> in GNU Binutils 2.28 has a use-after-free (specifically read-after-free) error while processing multiple, relocated sections, which allows remote attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-6969	<code>readelf</code> in GNU Binutils 2.28 is vulnerable to a heap-based buffer over-read while processing corrupt RL78 binaries, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file.

CVE-2017-7000	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted PDF file.
CVE-2017-7186	libpcre1 in PCRE 8.40 and libpcre2 in PCRE2 10.23 allow remote attackers to cause a denial of service (segmentation fault/crash) by triggering an invalid Unicode property lookup.
CVE-2017-7209	The dump_section_as_bytes function in readelf in GNU Binutils 2.28 accesses a NULL pointer while reading section headers, leading to a program crash.
CVE-2017-7210	objdump in GNU Binutils 2.28 is vulnerable to multiple heap-based buffer over-reads (of size 1 and size 8) while handling a crafted object file, leading to program crash.
CVE-2017-7223	GNU assembler in GNU Binutils 2.28 is vulnerable to a global buffer overflow (of size 1) while attempting to uncompress a section, potentially leading to a program crash.
CVE-2017-7224	The find_nearest_line function in objdump in GNU Binutils 2.28 is vulnerable to an invalid write (of size 1) while processing an empty function name, leading to a program crash.
CVE-2017-7225	The find_nearest_line function in addr2line in GNU Binutils 2.28 does not handle the case where the main file name is empty, triggering a NULL pointer dereference and an invalid write, and leading to a program crash.
CVE-2017-7226	The pe_ILF_object_p function in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an over-read of size 4049 because it uses the strlen function instead of strlen, leading to program crashes in several utilities, which could lead to information disclosure as well.
CVE-2017-7227	GNU linker (ld) in GNU Binutils 2.28 is vulnerable to a heap-based buffer overflow while processing a bogus input file, which relates to lack of '\0' termination of a name field in ldlex.l.
CVE-2017-7244	The _pcre32_xclass function in pcre_xclass.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (segmentation fault/crash) via a crafted file.
CVE-2017-7299	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an invalid read (of size 4) (bfd_elf_final_link function in bfd/elflink.c) does not check the format of the input file before trying to read the ELF header, which leads to a GNU linker (ld) program crash.
CVE-2017-7300	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an aout_link_add_section vulnerable to a heap-based buffer over-read (off-by-one) because of an incomplete check for invalid string offsets, leading to a linker (ld) program crash.
CVE-2017-7301	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an aout_link_add_section off-by-one vulnerability because it does not carefully check the string offset. The vulnerability could lead to a GNU linker (ld) program crash.
CVE-2017-7302	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has a swap_std_reloc_convert to an invalid read (of size 4) because of missing checks for relocations that could not be recognised. This vulnerability could lead to a linker (ld) program crash.
CVE-2017-7303	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read check (in the find_link function) for null headers before attempting to match them. This vulnerability causes Binutils linker (ld) program crash.
CVE-2017-7304	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read check (in the copy_special_section_fields function) for an invalid sh_link field before attempting to follow it. This vulnerability could lead to a crash.
CVE-2017-7375	A flaw in libxml2 allows remote XML entity inclusion with default parser flags (i.e., when the caller did not request noent, no_dtd_subset loading, or default DTD attributes). Depending on the context, this may expose a higher-risk attack surface, such as default parser flags, and expose content from local files, HTTP, or FTP servers (which might be otherwise unreachable).
CVE-2017-7407	The ourWriteOut function in tool_writeout.c in curl 7.53.1 might allow physically proximate attackers to obtain sensitive information under opportunistic circumstances by reading a workstation screen during use of a --write-out argument ending in a '%' character, leading to an over-read.
CVE-2017-7500	It was found that rpm did not properly handle RPM installations when a destination path was a symbolic link to a directory, and permissions of an arbitrary directory, and RPM files being placed in an arbitrary destination. An attacker, with write access to the subdirectory will be installed, could redirect that directory to an arbitrary location and gain root privilege.
CVE-2017-7501	It was found that versions of rpm before 4.13.0.2 use temporary files with predictable names when installing an RPM package in a directory where files will be installed could create symbolic links to an arbitrary location and modify content, and possibly could be used for denial of service or possibly privilege escalation.
CVE-2017-7526	libgcrypt before version 1.7.8 is vulnerable to a cache side-channel attack resulting into a complete break of RSA-1024 computing the sliding-window expansion. The same attack is believed to work on RSA-2048 with moderately more data. An attacker can run arbitrary software on the hardware where the private RSA key is used.
CVE-2017-7607	The handle_gnu_hash function in readelf.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap overflow/crash) via a crafted ELF file.

CVE-2017-7608	The <code>ebf_object_note_type_name</code> function in <code>eblobjnotetypename.c</code> in <code>elfutils</code> 0.168 allows remote attackers to cause a read and application crash) via a crafted ELF file.
CVE-2017-7609	<code>elf_compress.c</code> in <code>elfutils</code> 0.168 does not validate the zlib compression factor, which allows remote attackers to cause a crash via a crafted ELF file.
CVE-2017-7610	The <code>check_group</code> function in <code>elflint.c</code> in <code>elfutils</code> 0.168 allows remote attackers to cause a denial of service (heap-based overflow) via a crafted ELF file.
CVE-2017-7611	The <code>check_symtab_shndx</code> function in <code>elflint.c</code> in <code>elfutils</code> 0.168 allows remote attackers to cause a denial of service (heap-based overflow) via a crafted ELF file.
CVE-2017-7612	The <code>check_sysv_hash</code> function in <code>elflint.c</code> in <code>elfutils</code> 0.168 allows remote attackers to cause a denial of service (heap-based overflow) via a crafted ELF file.
CVE-2017-7613	<code>elflint.c</code> in <code>elfutils</code> 0.168 does not validate the number of sections and the number of segments, which allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file.
CVE-2017-7614	<code>elflink.c</code> in the Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.28, has a "member access" behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-7781	An error occurs in the elliptic curve point addition algorithm that uses mixed Jacobian-affine coordinates where it should not. A man-in-the-middle attacker could use this to interfere with a connection, resulting in an attack on the secret. This vulnerability affects Firefox < 55.
CVE-2017-7781	An error occurs in the elliptic curve point addition algorithm that uses mixed Jacobian-affine coordinates where it should not. A man-in-the-middle attacker could use this to interfere with a connection, resulting in an attack on the secret. This vulnerability affects Firefox < 55.
CVE-2017-8392	The Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read to determine whether symbols are NULL in the <code>_bfd_dwarf2_find_nearest_line</code> function. This vulnerability causes programs using the <code>libbfd</code> library, such as <code>objdump</code> , to crash.
CVE-2017-8393	The Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.28, is vulnerable to a global buffer overflow assumption made by code that runs for <code>objcopy</code> and <code>strip</code> , that <code>SHT_REL/SHR_RELA</code> sections are always named <code>__rela</code> . This vulnerability causes programs that conduct an analysis of binary programs using the <code>libbfd</code> library, such as <code>objcopy</code> , to crash.
CVE-2017-8394	The Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read dereferencing of <code>_bfd_elf_large_com_section</code> . This vulnerability causes programs that conduct an analysis of binary programs using the <code>libbfd</code> library, such as <code>objcopy</code> , to crash.
CVE-2017-8395	The Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read <code>malloc()</code> return-value check to see if memory had actually been allocated in the <code>_bfd_generic_get_section_contents</code> function. This vulnerability causes programs that conduct an analysis of binary programs using the <code>libbfd</code> library, such as <code>objcopy</code> , to crash.
CVE-2017-8396	The Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read offset range tests didn't catch small negative offsets less than the size of the reloc field. This vulnerability causes programs using the <code>libbfd</code> library, such as <code>objdump</code> , to crash.
CVE-2017-8397	The Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read size 1 during processing of a corrupt binary containing reloc(s) with negative addresses. This vulnerability causes programs using the <code>libbfd</code> library, such as <code>objdump</code> , to crash.
CVE-2017-8398	<code>dwarf.c</code> in GNU Binutils 2.28 is vulnerable to an invalid read of size 1 during dumping of debug information from binaries. This vulnerability causes programs that conduct an analysis of binary programs, such as <code>objdump</code> and <code>readelf</code> , to crash.
CVE-2017-8421	The function <code>coff_set_alignment_hook</code> in <code>coffcode.h</code> in Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.28, has a buffer overflow leak vulnerability which can cause memory exhaustion in <code>objdump</code> via a crafted PE file. Additional validation in <code>coffcode.h</code> is needed to resolve this.
CVE-2017-8804	The <code>xdr_bytes</code> and <code>xdr_string</code> functions in the GNU C Library (aka <code>glibc</code> or <code>libc6</code>) 2.25 mishandle failures of buffer allocation, which allows remote attackers to cause a denial of service (virtual memory allocation, or memory consumption if an overcommit setting is set to <code>111</code> , a related issue to CVE-2017-8779). NOTE: [Information provided from upstream and references]
CVE-2017-8817	The FTP wildcard function in <code>curl</code> and <code>libcurl</code> before 7.57.0 allows remote attackers to cause a denial of service (out-of-memory) via a string that ends with an <code>'</code> character.
CVE-2017-8872	The <code>htmlParseTryOrFinish</code> function in <code>HTMLparser.c</code> in <code>libxml2</code> 2.9.4 allows attackers to cause a denial of service (out-of-memory) via a crafted XML file.
CVE-2017-9038	GNU Binutils 2.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file. The <code>get_unwind_section_word</code> function in <code>readelf.c</code> , and ARM unwind offsets.

CVE-2017-9039	GNU Binutils 2.28 allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file that triggers a <code>get_program_headers</code> function in <code>readelf.c</code> .
CVE-2017-9040	GNU Binutils 2017-04-03 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file that triggers a large memory-allocation attempt in the <code>process_mips_specific</code> function in <code>readelf.c</code> .
CVE-2017-9041	GNU Binutils 2.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file that triggers a MIPS GOT mishandling in the <code>process_mips_specific</code> function in <code>readelf.c</code> .
CVE-2017-9042	<code>readelf.c</code> in GNU Binutils 2017-04-12 has a "cannot be represented in type long" issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-9043	<code>readelf.c</code> in GNU Binutils 2017-04-12 has a "shift exponent too large for type unsigned long" issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-9044	The <code>print_symbol_for_build_attribute</code> function in <code>readelf.c</code> in GNU Binutils 2017-04-12 allows remote attackers to cause a denial of service (application crash or SEGV) via a crafted ELF file.
CVE-2017-9047	A buffer overflow was discovered in <code>libxml2</code> 20904-GITv2.9.4-16-g0741801. The function <code>xmlSprintfElementContent</code> recursively dump the element content definition into a char buffer 'buf' of size 'size'. The variable <code>len</code> is assigned to the size of the content, then (i) the content->prefix is appended to buf (if it actually fits) when the content is not <code>XML_ELEMENT_CONTENT_ELEMENT</code> , then (ii) the content->name is appended to buf (if it actually fits) when the content is <code>XML_ELEMENT_CONTENT_ELEMENT</code> . However, the check for whether the content->name actually fits also uses 'len' rather than the updated buffer size. This vulnerability causes programs that use <code>libxml2</code> , such as PHP, to crash.
CVE-2017-9048	<code>libxml2</code> 20904-GITv2.9.4-16-g0741801 is vulnerable to a stack-based buffer overflow. The function <code>xmlSprintfElementContent</code> recursively dump the element content definition into a char buffer 'buf' of size 'size'. At the end of the routine, the function checks whether the current <code>strlen(buf) + 2 < size</code> . This vulnerability causes programs that use <code>libxml2</code> , such as PHP, to crash.
CVE-2017-9049	<code>libxml2</code> 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the <code>xmlDictComputeFast</code> function. This vulnerability exists because of an incomplete fix for CVE-2017-9047. This vulnerability causes programs that use <code>libxml2</code> , such as PHP, to crash.
CVE-2017-9050	<code>libxml2</code> 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the <code>xmlDictAddString</code> function. This vulnerability exists because of an incomplete fix for CVE-2017-9047. This vulnerability causes programs that use <code>libxml2</code> , such as PHP, to crash.
CVE-2017-9233	XML External Entity vulnerability in <code>libexpat</code> 2.2.0 and earlier (Expat XML Parser Library) allows attackers to put a malformed external entity definition from an external DTD.
CVE-2017-9742	The <code>score_opcodes</code> function in <code>opcodes/score7-dis.c</code> in GNU Binutils 2.28 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9743	The <code>print_insn_score32</code> function in <code>opcodes/score7-dis.c:552</code> in GNU Binutils 2.28 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9744	The <code>sh_elf_set_mach_from_flags</code> function in <code>bfd/elf32-sh.c</code> in the Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9745	The <code>_bfd_vms_slurp_etir</code> function in <code>bfd/vms-alpha.c</code> in the Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9746	The <code>disassemble_bytes</code> function in <code>objdump.c</code> in GNU Binutils 2.28 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of rae insns pri during "objdump -D" execution.
CVE-2017-9747	The <code>ieee_archive_p</code> function in <code>bfd/ieee.c</code> in the Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. NOTE: this may be related to a compiler bug.
CVE-2017-9748	The <code>ieee_object_p</code> function in <code>bfd/ieee.c</code> in the Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. NOTE: this may be related to a compiler bug.
CVE-2017-9749	The <code>*regs*</code> macros in <code>opcodes/bfin-dis.c</code> in GNU Binutils 2.28 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9750	<code>opcodes/rx-decode.opc</code> in GNU Binutils 2.28 lacks bounds checks for certain scale arrays, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9751	<code>opcodes/rl78-decode.opc</code> in GNU Binutils 2.28 has an unbounded GETBYTE macro, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.

CVE-2017-9752	bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9753	The versados_mkobject function in bfd/versados.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9754	The process_otr function in bfd/versados.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9755	opcodes/i386-dis.c in GNU Binutils 2.28 does not consider the number of registers for bnd mode, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9756	The aarch64_ext_ldst_reglist function in opcodes/aarch64-dis.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9954	The getvalue function in tekhex.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (stack-based buffer over-read and application crash) via a crafted tekhex file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9955	The get_build_id function in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file in which a certain size field, as demonstrated by mishandling within the objdump program.
CVE-2018-1000030	Python 2.7.14 is vulnerable to a Heap-Buffer-Overflow as well as a Heap-Use-After-Free. Python versions prior to 2.7.14 are vulnerable to a Heap-Buffer-Overflow as well as a Heap-Use-After-Free. Python versions 2.7.14 and prior may also be vulnerable however this has not been confirmed. The vulnerability lies within the Thread1 object. In both cases there is essentially a race condition that occurs. For the Heap-Buffer-Overflow, Thread1 is already writing to the buffer without knowing how much to write. So when a large amount of data is being written, it causes a corruption using a Heap-Buffer-Overflow. As for the Use-After-Free, Thread3->Malloc->Thread1->Free's->Thread1 is already free. The vulnerability is stated that this is not a security vulnerability due to the fact that the attacker must be able to run code, however in some cases this vulnerability can potentially be used by an attacker to violate a trust boundary, as such the DWF feels this issue should be tracked as a security vulnerability.
CVE-2018-1058	A flaw was found in the way PostgreSQL allowed a user to modify the behavior of a query for other users. An attacker could execute code with the permissions of superuser in the database. Versions 9.3 through 10 are affected.
CVE-2018-10754	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was not accepted because it did not show that it was not a security issue.  Note: None.
CVE-2018-11212	An issue was discovered in libjpeg 9a and 9d. The alloc_sarray function in jmemmgr.c allows remote attackers to cause a denial of service (buffer overflow and application crash) via a crafted file.
CVE-2018-1123	procps-ng before version 3.3.15 is vulnerable to a denial of service in ps via mmap buffer overflow. Inbuilt protection is present, ensuring that the impact of this flaw is limited to a crash (temporary denial of service).
CVE-2018-1125	procps-ng before version 3.3.15 is vulnerable to a stack buffer overflow in pgrep. This vulnerability is mitigated by a patch that checks for a null allocated string. When pgrep is compiled with FORTIFY (as on Red Hat Enterprise Linux and Fedora), the impact is limited to a crash (temporary denial of service).
CVE-2018-13785	In libpng 1.6.34, a wrong calculation of row_factor in the png_check_chunk_length function (pngutil.c) may trigger a buffer overflow by-zero while processing a crafted PNG file, leading to a denial of service.
CVE-2018-16375	An issue was discovered in OpenJPEG 2.3.0. Missing checks for header_info.height and header_info.width in the fct function can lead to a heap-based buffer overflow.
CVE-2018-16429	GNOME GLib 2.56.1 has an out-of-bounds read vulnerability in g_markup_parse_context_parse() in gmarkup.c, which allows remote attackers to cause a denial of service (buffer overflow and application crash) via a crafted XML file.
CVE-2018-18508	In Network Security Services (NSS) before 3.36.7 and before 3.41.1, a malformed signature can cause a crash due to a buffer overflow in the signature verification process.
CVE-2018-18508	In Network Security Services (NSS) before 3.36.7 and before 3.41.1, a malformed signature can cause a crash due to a buffer overflow in the signature verification process.
CVE-2018-20482	GNU Tar through 1.30, when --sparse is used, mishandles file shrinkage during read access, which allows local users to cause a denial of service (buffer overflow and application crash) by modifying a file that is supposed to be archived by a different user's program.
CVE-2018-25032	zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant non-zero values.

CVE-2018-2938	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Java DB). Supported versions that are affected are 8u172. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data and components. This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java applets, such as through a web service. CVE-2018-2938 addresses CVE-2018-1313. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).
CVE-2018-2940	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data and components. This vulnerability typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/I:N/A:N).
CVE-2018-2952	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171; JRockit: R28.3.18. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets. It can also be exploited through sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2018-2973	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, modification or deletion of data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).
CVE-2018-3136	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.4 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N).
CVE-2018-3139	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data and components. This vulnerability typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2018-3149	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component to supply data to the APIs. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).
CVE-2018-3169	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data and components. This vulnerability typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).

CVE-2018-3180	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JSSE). Successful attacks of this vulnerability allow an attacker to gain network access via SSL/TLS to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized read or insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized read or delete access to some of Java SE, Java SE Embedded, JRockit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 9.0 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L).
CVE-2018-3183	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Scripting). Successful attacks of this vulnerability allow an attacker to gain network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, it can significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 9.0 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).
CVE-2018-3214	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Sound). Successful attacks of this vulnerability allow an attacker to gain network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, it can significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).
CVE-2018-3639	Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the results are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel attack. Variant 4.
CVE-2018-6003	An issue was discovered in the _asn1_decode_simple_ber function in decoding.c in GNU Libtasn1 before 4.13. Unauthenticated attackers could cause a stack exhaustion and DoS.
CVE-2018-6323	The elf_object_p function in elfcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils through 2.30, allows a remote attacker to cause a denial of service (DoS) via a buffer overflow because bfd_size_type multiplication is not used. A crafted ELF file allows remote attackers to cause a denial of service (DoS) and have unspecified other impact.
CVE-2018-6759	The bfd_get_debug_link_info_1 function in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils through 2.30, allows a remote attacker to cause a denial of service (DoS) via an unchecked strlen operation. Remote attackers could leverage this vulnerability to cause a denial of service (DoS) and have unspecified other impact.
CVE-2018-6829	Libgcrypt through 1.8.2, when used to encrypt messages directly, improperly encodes plaintext data into ciphertext information by reading ciphertext data (i.e., it does not have semantic security in face of a ciphertext-only attack). This is because the underlying assumption does not hold for Libgcrypt's ElGamal implementation.
CVE-2018-6954	systemd-tmpfiles in systemd through 237 mishandles symlinks present in non-terminal path components, which allows an attacker to create arbitrary files via vectors involving creation of a directory and a file under that directory, and later replacing that directory with a symlink. NOTE: this issue only exists if the fs.protected_symlinks sysctl is turned on.
CVE-2018-8740	In SQLite through 3.22.0, databases whose schema is corrupted using a CREATE TABLE AS statement could cause a denial of service (DoS) via a buffer overflow in build.c and prepare.c.
CVE-2018-9234	GnuPG 2.2.4 and 2.2.5 does not enforce a configuration in which key certification requires an offline master Certification. This allows an attacker to create certifications that occurred only with access to a signing subkey.
CVE-2019-11191	The Linux kernel through 5.0.7, when CONFIG_IA32_AOUT is enabled and ia32_aout is loaded, allows local users to cause a denial of service (DoS) via a buffer overflow (if any exist) because install_exec_creds() is called too late in load_aout_binary() in fs/binfmt_aout.c, and thus the condition when reading /proc/pid/stat. NOTE: the software maintainer disputes that this is a vulnerability because AOUT has not been supported.
CVE-2019-12378	An issue was discovered in ip6_ra_control in net/ipv6/ipv6_sockglue.c in the Linux kernel through 5.1.5. There is a NULL pointer dereference which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). NOTE: This has been fixed in the Linux kernel through 5.1.6.
CVE-2019-12379	An issue was discovered in con_insert_unipair in drivers/tty/vt/consolemap.c in the Linux kernel through 5.1.5. There is a NULL pointer dereference which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). NOTE: This id is disputed as not being an issue.
CVE-2019-12381	An issue was discovered in ip_ra_control in net/ipv4/ip_sockglue.c in the Linux kernel through 5.1.5. There is a NULL pointer dereference which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). NOTE: this is disputed as not being an issue.
CVE-2019-12382	An issue was discovered in drm_load_edid_firmware in drivers/gpu/drm/drm_edid_load.c in the Linux kernel through 5.1.5. There is a NULL pointer dereference which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). NOTE: this is disputed as not being a vulnerability because kstrdup() returning NULL is handled sufficiently and there is no chance for a NULL pointer dereference.


CVE-2019-12455	An issue was discovered in sunxi_divs_clk_setup in drivers/clk/sunxi/clk-sunxi.c in the Linux kernel through 5.1.5 derived_name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash) because the memory allocation that was not checked is part of a code that only runs at boot time, before the kernel is initialized. This is not a denial of service, but it is no possibility for an unprivileged user to control it, and no denial of service.
CVE-2019-12456	An issue was discovered in the MPT3COMMAND case in _ctl_ioctl_main in drivers/scsi/mpt3sas/mpt3sas_ctl.c in the Linux kernel through 5.1.5. Local users can cause a denial of service or possibly have unspecified other impact by changing the value of ioc_num to a "double fetch" vulnerability. NOTE: a third party reports that this is unexploitable because the doubly fetched value is not used.
CVE-2019-13012	The keyfile settings backend in GNOME GLib (aka glib2.0) before 2.60.0 creates directories using g_file_make_directory_with_parents (which creates the directory and its parents) and files using g_file_replace_contents (kfsb->file, contents, length, NULL, FALSE, G_FILE_CREATE_REPLACE_EXISTING, NULL). Consequently, it does not properly restrict directory (and file) permissions. Instead, for directories, 0777 permissions are used. This is similar to CVE-2019-12450.
CVE-2019-13050	Interaction between the sks-keyserver code through 1.2.0 of the SKS keyserver network, and GnuPG through 2.2.19. Configuration line referring to a host on the SKS keyserver network. Retrieving data from this network may cause a Certificate Spamming Attack.
CVE-2019-13057	An issue was discovered in the server in OpenLDAP before 2.4.48. When the server administrator delegates rootDN to a database but wants to maintain isolation (e.g., for multi-tenant deployments), slapd does not properly stop a rootDN from another database during a SASL bind or with a proxyAuthz (RFC 4370) control. (It is not a common configuration for a server administrator and a DB administrator enjoy different levels of trust.)
CVE-2019-13565	An issue was discovered in OpenLDAP 2.x before 2.4.48. When using SASL authentication and session encryption in slapd access controls, it is possible to obtain access that would otherwise be denied via a simple bind for any identifier. After a SASL bind is completed, the sasl_ssf value is retained for all new non-SASL connections. Depending on the ACL configuration, operations (searches, modifications, etc.). In other words, a successful authorization step completed by one user can be used by a different user.
CVE-2019-13751	Uninitialized data in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentially sensitive information via a crafted HTML page.
CVE-2019-13752	Out of bounds read in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentially sensitive information via a crafted HTML page.
CVE-2019-13753	Out of bounds read in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentially sensitive information via a crafted HTML page.
CVE-2019-16231	drivers/net/fjes/fjes_main.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a denial of service (kernel crash) via a crafted network packet.
CVE-2019-16232	drivers/net/wireless/marvell/libertas/if_sdio.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a denial of service (kernel crash) via a crafted network packet.
CVE-2019-16233	drivers/scsi/qla2xxx/qla_os.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a denial of service (kernel crash) via a crafted network packet.
CVE-2019-16234	drivers/net/wireless/intel/iwlwifi/pcie/trans.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a denial of service (kernel crash) via a crafted network packet.
CVE-2019-16276	Go before 1.12.10 and 1.13.x before 1.13.1 allow HTTP Request Smuggling.
CVE-2019-16276	Go before 1.12.10 and 1.13.x before 1.13.1 allow HTTP Request Smuggling.
CVE-2019-17450	find_abstract_instance in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32, allows a local user to cause a denial of service (infinite recursion and application crash) via a crafted ELF file.
CVE-2019-17451	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. A local user can cause a denial of service (infinite recursion and application crash) via a crafted ELF file. This is similar to the CVE-2019-9740 query string issue and the CVE-2019-9947 path string issue. (This is not expected to be fixed.) This is fixed in: v2.7.18, v2.7.18rc1; v3.5.10, v3.5.10rc1; v3.6.11, v3.6.11rc1, v3.6.12; v3.7.8, v3.7.8rc1, v3.7.9, v3.7.9rc1, v3.8.5, v3.8.6, v3.8.6rc1.
CVE-2019-17594	There is a heap-based buffer over-read in the _nc_find_entry function in tinfo/comp_hash.c in the terminfo library in ncurses through 6.2.
CVE-2019-17595	There is a heap-based buffer over-read in the fmt_entry function in tinfo/comp_hash.c in the terminfo library in ncurses through 6.2.
CVE-2019-18276	An issue was discovered in disable_priv_mode in shell.c in GNU Bash through 5.0 patch 11. By default, if Bash is running as root, it will drop privileges by setting its effective UID to its real UID. However, it does so incorrectly. On Linux and macOS, the saved UID is not dropped. An attacker with command execution in the shell can use "enable -f" to enable a shared object that calls setuid(0) and therefore regains privileges. However, binaries running with an effective UID of 0 are not affected.
CVE-2019-18348	An issue was discovered in urllib2 in Python 2.x through 2.7.17 and urllib in Python 3.x through 3.8.0. CRLF injection in the request parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the host component of the URL). This is similar to the CVE-2019-9740 query string issue and the CVE-2019-9947 path string issue. (This is not expected to be fixed.) This is fixed in: v2.7.18, v2.7.18rc1; v3.5.10, v3.5.10rc1; v3.6.11, v3.6.11rc1, v3.6.12; v3.7.8, v3.7.8rc1, v3.7.9, v3.7.9rc1, v3.8.5, v3.8.6, v3.8.6rc1.

CVE-2019-19070	A memory leak in the <code>spi_gpio_probe()</code> function in <code>drivers/spi/spi-gpio.c</code> in the Linux kernel through 5.3.11 allows (memory consumption) by triggering <code>devm_add_action_or_reset()</code> failures, aka CID-d3b0ffa1d75d. NOTE: third party system must have already been out of memory before the probe began
CVE-2019-19449	In the Linux kernel 5.0.21, mounting a crafted <code>f2fs</code> filesystem image can lead to slab-out-of-bounds read access in <code>segment.c</code> , related to <code>init_min_max_mtime</code> in <code>fs/f2fs/segment.c</code> (because the second argument to <code>get_seg_entry</code> is null)
CVE-2019-19603	SQLite 3.30.1 mishandles certain <code>SELECT</code> statements with a nonexistent <code>VIEW</code> , leading to an application crash.
CVE-2019-19645	<code>alter.c</code> in SQLite through 3.30.1 allows attackers to trigger infinite recursion via certain types of self-referential view statements.
CVE-2019-19880	<code>exprListAppendList</code> in <code>window.c</code> in SQLite 3.30.1 allows attackers to trigger an invalid pointer dereference because clauses of window definitions are mishandled.
CVE-2019-19906	<code>cyrus-sasl</code> (aka Cyrus SASL) 2.1.27 has an out-of-bounds write leading to unauthenticated remote denial-of-service packet. The OpenLDAP crash is ultimately caused by an off-by-one error in <code>_sasl_add_string</code> in <code>common.c</code> in <code>cyrus-sasl</code>
CVE-2019-19924	SQLite 3.30.1 mishandles certain parser-tree rewriting, related to <code>expr.c</code> , <code>vdbeaux.c</code> , and <code>window.c</code> . This is caused by <code>ExprListRewrite</code> handling.
CVE-2019-20218	<code>selectExpander</code> in <code>select.c</code> in SQLite 3.30.1 proceeds with <code>WITH</code> stack unwinding even after a parsing error.
CVE-2019-20387	<code>repodata_schema2id</code> in <code>repodata.c</code> in <code>libsolv</code> before 0.7.6 has a heap-based buffer over-read via a last schema whose schema.
CVE-2019-2422	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are 11.0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code that comes from the Java runtime). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N)
CVE-2019-2426	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are 11.0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N)
CVE-2019-2602	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by using APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVE-2019-2684	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, modification or deletion of critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N)
CVE-2019-2698	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are 11.0.1; Java SE Embedded: 8u191. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code that comes from the Java runtime). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N)
CVE-2019-2708	Vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are Prior to 5.3.22. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure to compromise Data Store. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (DoS) to the Data Store. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:N)

CVE-2019-2745	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are 7u221, 8u212, 11.0.3 and 12.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE is installed to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE data. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2019-2762	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supported versions that are affected are 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2019-2766	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N).
CVE-2019-2769	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supported versions that are affected are 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2019-2786	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Attacks of this vulnerability may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2019-2816	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2019-2842	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JCE). The supported version that is affected is 8u212. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2019-2894	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions that are affected are 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).

CVE-2019-2933	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. This vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/UI:R/S:U/C:L/T:N/A:N).
CVE-2019-2945	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. This vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/T:N/A:L).
CVE-2019-2949	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). Supported versions: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may succeed on Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/T:N/A:N).
CVE-2019-2958	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, modification or deletion of critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2962	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2964	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Supported versions: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2973	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2975	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insertion or deletion of Java SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L).

CVE-2019-2978	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2981	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2983	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2987	Vulnerability in the Java SE product of Oracle Java SE (component: 2D). Supported versions that are affected are 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running or sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2988	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code that comes from the internet). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2989	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical accessible data. Note: This vulnerability applies to Java deployments, typically in clients running or sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2992	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running or sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code that comes from the internet). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2999	Vulnerability in the Java SE product of Oracle Java SE (component: Javadoc). Supported versions that are affected are 8u221, 11.0.4 and 13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running or sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code that comes from the internet). CVSS 3.0 Base Score 4.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-3842	In systemd before v242-rc4, it was discovered that pam_systemd does not properly sanitize the environment before an attacker, in some particular configurations, to set a XDG_SEAT environment variable which allows for compromise of the system using the "allow_active" element rather than "allow_any".
CVE-2019-3859	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the _libssh2_packet_require and _libssh2_packet_read functions. An attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.

CVE-2019-3860	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SFTP packets with empty payloads are handled. An attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-5827	Integer overflow in SQLite via WebSQL in Google Chrome prior to 74.0.3729.131 allowed a remote attacker to potentially crash the browser or execute arbitrary code.
CVE-2019-9074	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32.1. A remote attacker could cause a Denial of Service (DoS) via a crafted ELF file, which triggers a SEGV in bfd_getl32 in libbfd.c, when called from pex64_get_runtime_function in pei-x86_64.c.
CVE-2020-11725	snd_ctl_elem_add in sound/core/control.c in the Linux kernel through 5.6.3 has a count=info->owner line, which leads to a multiplication for unspecified "interesting side effects." NOTE: kernel engineers dispute this finding, because it could not be reproduced. It was added that were unfamiliar with the misuse of the info->owner field to represent data unrelated to the "owner" of the SPCR_IOCTL_ELEM_ADD and SPCR_IOCTL_ELEM_REPLACE, have been designed to misuse the field.
CVE-2020-12762	json-c through 0.14 has an integer overflow and out-of-bounds write via a large JSON file, as demonstrated by prime512.json.
CVE-2020-13435	SQLite through 3.32.0 has a segmentation fault in sqlite3ExprCodeTarget in expr.c.
CVE-2020-13631	SQLite before 3.32.0 allows a virtual table to be renamed to the name of one of its shadow tables, related to alter table.
CVE-2020-13776	systemd through v245 mishandles numerical usernames such as ones composed of decimal digits or 0x followed by a digit, which can lead to a Denial of Service (DoS) or privilege escalation when privileges of the 0x0 user account were intended.  Note: This issue exists because of an incomplete fix for CVE-2017-1000082.
CVE-2020-14155	libpcre in PCRE before 8.44 allows an integer overflow via a large number after a (?C substring.
CVE-2020-14350	It was found that some PostgreSQL extensions did not use search_path safely in their installation script. An attacker could trick an administrator into executing a specially crafted script, during the installation or update of such extension. The affected versions are 12.4, before 11.9, before 10.14, before 9.6.19, and before 9.5.23.
CVE-2020-14556	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions: 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, deletion, or creation of data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/AT:N/Au/C:U/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14577	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions: 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/AT:N/Au/C:U/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14578	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions: 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (DoS) to Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/AT:N/Au/C:U/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14579	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions: 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (DoS) to Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/AT:N/Au/C:U/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14581	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions: 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/AT:N/Au/C:U/PR:N/UI:N/S:U/C:L/I:N/A:N).

CVE-2020-14583	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in client applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and that rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N).
CVE-2020-14593	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code installed by an administrator). CVSS 3.1 Base Score 7.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N).
CVE-2020-14621	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component and Interface. It can also be exploited by supplying data to APIs in the specified Component and Interface using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14779	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions: 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized access to critical data or all Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited by supplying data to APIs in the specified Component and Interface. It can also be exploited by supplying data to APIs in the specified Component and Interface using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14781	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JNDI). Supported versions: 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited by supplying data to APIs in the specified Component and Interface. It can also be exploited by supplying data to APIs in the specified Component and Interface using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14782	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions: 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited by supplying data to APIs in the specified Component and Interface. It can also be exploited by supplying data to APIs in the specified Component and Interface using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14792	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Hotspot). Supported versions: 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited by supplying data to APIs in the specified Component and Interface. It can also be exploited by supplying data to APIs in the specified Component and Interface using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N).
CVE-2020-14796	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions: 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited by supplying data to APIs in the specified Component and Interface. It can also be exploited by supplying data to APIs in the specified Component and Interface using Untrusted Java Web Start applications or Untrusted Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N).

CVE-2020-14797	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions: 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited by supplying data to APIs in the specified Component, e.g., through a web service which runs Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component, e.g., through a web service which runs Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14798	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions: 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. This vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited by supplying data to APIs in the specified Component, e.g., through a web service which runs Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component, e.g., through a web service which runs Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14803	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affected: 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability can be exploited by supplying data to APIs in the specified Component, e.g., through a web service which runs clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-16590	A double free vulnerability exists in the Binary File Descriptor (BFD) (aka libbfd) in GNU Binutils 2.35 in the process of reading a file via a crafted file.
CVE-2020-16591	A Denial of Service vulnerability exists in the Binary File Descriptor (BFD) in GNU Binutils 2.35 due to an invalid read access to memory demonstrated in readelf.
CVE-2020-16592	A use after free issue exists in the Binary File Descriptor (BFD) library (aka libbfd) in GNU Binutils 2.34 in bfd_h_open. This can cause a denial of service via a crafted file.
CVE-2020-16593	A Null Pointer Dereference vulnerability exists in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in binutils-2.35, in scan_unit_for_symbols, as demonstrated in addr2line, that can cause a denial of service via a crafted file.
CVE-2020-16599	A Null Pointer Dereference vulnerability exists in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in binutils-2.35, in _bfd_elf_get_symbol_version_string, as demonstrated in nm-new, that can cause a denial of service via a crafted file.
CVE-2020-16845	Go before 1.13.15 and 14.x before 1.14.7 can have an infinite read loop in ReadUvarint and ReadVarint in encoding.
CVE-2020-16845	Go before 1.13.15 and 14.x before 1.14.7 can have an infinite read loop in ReadUvarint and ReadVarint in encoding.
CVE-2020-21583	An issue was discovered in hwclock.13-v2.27 allows attackers to gain escalated privileges or execute arbitrary commands by exploiting a buffer overflow in the date.
CVE-2020-22218	An issue was discovered in function _libssh2_packet_add in libssh2 1.10.0 allows attackers to access out of bounds memory.
CVE-2020-24553	Go before 1.14.8 and 1.15.x before 1.15.1 allows XSS because text/html is the default for CGI/FCGI handlers that do not set the Content-Type header.
CVE-2020-24736	Buffer Overflow vulnerability found in SQLite3 v.3.27.1 and before allows a local attacker to cause a denial of service.
CVE-2020-24977	GNOME project libxml2 v2.9.10 has a global buffer over-read vulnerability in xmlEncodeEntitiesInternal at libxml2-2.9.10 commit 50f06b3e.
CVE-2020-25696	A flaw was found in the psql interactive terminal of PostgreSQL in versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.24, before 9.5.24. If an interactive psql session uses \gset when querying a compromised server, the attacker can execute arbitrary SQL commands on the server. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-2583	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized access to confidential and/or protected data (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which runs Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-2590	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions: 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which runs Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).


CVE-2020-2593	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-2601	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may succeed on Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).
CVE-2020-2604	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS v3.0 Base Score 8.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-2654	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affected: 7u241, 8u231, 11.0.5 and 13.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java Web Start applications. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:L).
CVE-2020-2659	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions: 7u241 and 8u231; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxes, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-27216	In Eclipse Jetty versions 1.0 thru 9.4.32.v20200930, 10.0.0.alpha1 thru 10.0.0.beta2, and 11.0.0.alpha1 thru 11.0.0.beta2, a temporary directory is shared between all users on that system. A collocated user can observe the process of creating a temporary directory and race to complete the creation of the temporary subdirectory. If the attacker wins the race then the attacker can write to the subdirectory used to unpack web applications, including their WEB-INF/lib jar files and JSP files. If any code is executed in the subdirectory, this can lead to a local privilege escalation vulnerability.
CVE-2020-27218	In Eclipse Jetty version 9.4.0.RC0 to 9.4.34.v20201102, 10.0.0.alpha0 to 10.0.0.beta2, and 11.0.0.alpha0 to 11.0.0.beta2, if a request body is enabled and requests from different clients are multiplexed onto a single connection, and if an attacker can send a request that is not consumed by the application, then a subsequent request on the same connection will see that body prepended to its own body. An attacker can exploit this to inject data into the body of the subsequent request.
CVE-2020-27223	In Eclipse Jetty 9.4.6.v20170531 to 9.4.36.v20210114 (inclusive), 10.0.0, and 11.0.0 when Jetty handles a request with a large number of ,Äüquality,Äü (i.e. q) parameters, the server may enter a denial of service (DoS) state due to high CPU usage resulting in minutes of CPU time exhausted processing those quality values.
CVE-2020-2754	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions: 7u241, 8u231, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can also be exploited by supplying data to APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2755	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions: 7u241, 8u231, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can also be exploited by supplying data to APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).

CVE-2020-2756	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a Denial of Service (DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited by supplying data to APIs in the specified Component without using Untrusted Code. Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using Untrusted Code. Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2757	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a Denial of Service (DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited by supplying data to APIs in the specified Component without using Untrusted Code. Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using Untrusted Code. Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2773	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a Denial of Service (DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited by supplying data to APIs in the specified Component without using Untrusted Code. Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using Untrusted Code. Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2781	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Easily exploitable vulnerability allows unauthenticated attacker with network access to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial Denial of Service (DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through the network by supplying data to APIs in the specified Component without using Untrusted Code. Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using Untrusted Code. Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2800	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Code. Start applications and sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-2803	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. In Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. In Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator), this vulnerability does not apply. Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-2805	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. In Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. In Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator), this vulnerability does not apply. Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-28196	MIT Kerberos 5 (aka krb5) before 1.17.2 and 1.18.x before 1.18.3 allows unbounded recursion via an ASN.1-encoding issue. The asn1_encode.c support for BER indefinite lengths lacks a recursion limit.
CVE-2020-2830	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Supported versions: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Easily exploitable vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a Denial of Service (DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited by supplying data to APIs in the specified Component without using Untrusted Code. Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using Untrusted Code. Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-28362	Go before 1.14.12 and 1.15.x before 1.15.4 allows Denial of Service.

CVE-2020-28366	Code injection in the go command with cgo before Go 1.14.12 and Go 1.15.5 allows arbitrary code execution at build time by using a name in a linked object file.
CVE-2020-28367	Code injection in the go command with cgo before Go 1.14.12 and Go 1.15.5 allows arbitrary code execution at build time by using a #cgo directive.
CVE-2020-29361	An issue was discovered in p11-kit 0.21.1 through 0.23.21. Multiple integer overflows have been discovered in the p11-kit list command, where overflow checks are missing before calling realloc or calloc.
CVE-2020-29362	An issue was discovered in p11-kit 0.21.1 through 0.23.21. A heap-based buffer over-read has been discovered in the remote commands and the client library. When the remote entity supplies a byte array through a serialized PKCS#11 object, allow the reading of up to 4 bytes of memory past the heap allocation.
CVE-2020-35448	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.35.1. A buffer overflow occurs in bfd_getl_signed_32 in libbfd.c because sh_entsize is not validated in _bfd_elf_slurp_secondary_reloc_section.
CVE-2020-35525	In SQLite 3.31.1, a potential null pointer dereference was found in the INTERSECT query processing.
CVE-2020-35527	In SQLite 3.31.1, there is an out of bounds access problem through ALTER TABLE for views that have a nested FROM clause.
CVE-2020-36221	An integer underflow was discovered in OpenLDAP before 2.4.57 leading to slapd crashes in the Certificate Exact Match service (schema_init.c serialNumberAndIssuerCheck).
CVE-2020-36222	A flaw was discovered in OpenLDAP before 2.4.57 leading to an assertion failure in slapd in the saslAuthzToValid service.
CVE-2020-36223	A flaw was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Values Return Filter control handling (free and out-of-bounds read).
CVE-2020-36224	A flaw was discovered in OpenLDAP before 2.4.57 leading to an invalid pointer free and slapd crash in the saslAuthzToValid service.
CVE-2020-36225	A flaw was discovered in OpenLDAP before 2.4.57 leading to a double free and slapd crash in the saslAuthzToValid service.
CVE-2020-36226	A flaw was discovered in OpenLDAP before 2.4.57 leading to a memch->bv_len miscalculation and slapd crash in the saslAuthzToValid service.
CVE-2020-36227	A flaw was discovered in OpenLDAP before 2.4.57 leading to an infinite loop in slapd with the cancel_extop Cancel operation.
CVE-2020-36228	An integer underflow was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Certificate List Entry service.
CVE-2020-36229	A flaw was discovered in ldap_X509dn2bv in OpenLDAP before 2.4.57 leading to a slapd crash in the X.509 DN parsing service.
CVE-2020-36230	A flaw was discovered in OpenLDAP before 2.4.57 leading to an assertion failure in slapd in the X.509 DN parsing service.
CVE-2020-36694	An issue was discovered in netfilter in the Linux kernel before 5.10. There can be a use-after-free in the packet protocol sequence count is mishandled during concurrent iptables rules replacement. This could be exploited with the CAP_NET_ADMIN namespace. NOTE: cc00bca was reverted in 5.12.
CVE-2020-8231	Due to use of a dangling pointer, libcurl 7.29.0 through 7.71.1 can use the wrong connection when sending data.
CVE-2020-8284	A malicious server can use the FTP PASV response to trick curl 7.73.0 and earlier into connecting back to a given IP address and make curl extract information about services that are otherwise private and not disclosed, for example doing port scans.
CVE-2020-8285	curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard file listing.
CVE-2020-8991	vg_lookup in daemons/lvmetad/lvmetad-core.c in LVM2 2.02 mismanages memory, leading to an lvmetad memory leak. NOTE: RedHat disputes CVE-2020-8991 as not being a vulnerability since there is no apparent route to either privilege escalation or denial of service through the bug.
CVE-2021-20197	There is an open race window when writing output in the following utilities in GNU binutils version 2.35 and earlier: objcopy, objdump, readelf, and strip. If these utilities are run as a privileged user (presumably as part of a script updating binaries across different users), an unprivileged user can get ownership of arbitrary files through a symlink.
CVE-2021-20229	A flaw was found in PostgreSQL in versions before 13.2. This flaw allows a user with SELECT privilege on one column to read all columns of the table. The highest threat from this vulnerability is to confidentiality.
CVE-2021-20266	A flaw was found in RPM's hdrblobInit() in lib/header.c. This flaw allows an attacker who can modify the rpmdb to cause a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2021-20294	A flaw was found in binutils readelf 2.35 program. An attacker who is able to convince a victim using readelf to read a file can cause a buffer overflow, out-of-bounds write of arbitrary data supplied by the attacker. The highest impact of this flaw is to confidentiality.

CVE-2021-22876	curl 7.1.1 to and including 7.75.0 is vulnerable to an "Exposure of Private Personal Information to an Unauthorized Referer: header. libcurl does not strip off user credentials from the URL when automatically populating the Referer: HTTP requests, and therefore risks leaking sensitive data to the server that is the target of the second HTTP request."
CVE-2021-22898	curl 7.7 through 7.76.1 suffers from an information disclosure when the <code>-t</code> command line option, known as <code>CURL</code> , is used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending <code>NEW_ENV</code> uninitialized data from a stack based buffer to the server, resulting in potentially revealing sensitive internal information over the protocol.
CVE-2021-22924	libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse, if one of them matches the config matching function did not take 'issuercert' into account and it compared the involved paths *case insensitive*. File paths are, or can be, case sensitive on many systems but not all, and can even vary depending on the platform. This includes the 'issuer cert' which a transfer can set to qualify how to verify the server certificate.
CVE-2021-22925	curl supports the <code>-t</code> command line option, known as <code>CURLOPT_TELNETOPTIONS</code> in libcurl. This rarely used option is used to send TELNET servers. Due to a flaw in the option parser for sending <code>NEW_ENV</code> variables, libcurl could be made to pass uninitialized data to the server. Therefore potentially revealing sensitive internal information to the server using a clear-text network protocol. It did not call and use <code>scanf()</code> correctly when parsing the string provided by the application.
CVE-2021-22946	A user can tell curl >= 7.20.0 and <= 7.78.0 to require a successful upgrade to TLS when speaking to an IMAP, POP3 or NNTP server by setting the command line or <code>CURLOPT_USE_SSL</code> set to <code>CURLUSESSL_CONTROL</code> or <code>CURLUSESSL_ALL</code> with libcurl. If the server would return a properly crafted but perfectly legitimate response. This flaw would then make curl silently accept the response contrary to the instructions and expectations, exposing possibly sensitive data in clear text over the network.
CVE-2021-22947	When curl >= 7.20.0 and <= 7.78.0 connects to an IMAP or POP3 server to retrieve data using STARTTLS to upgrade the connection and send back multiple responses at once that curl caches. curl would then upgrade to TLS but not flush the in-queue responses using and trusting the responses it got *before* the TLS handshake as if they were authenticated. Using this flaw, it is possible to inject the fake responses, then pass-through the TLS traffic from the legitimate server and trick curl into sending data. The injected data comes from the TLS-protected server.
CVE-2021-23214	When the server is configured to use trust authentication with a clientcert requirement or to use cert authentication, curl can execute arbitrary SQL queries when a connection is first established, despite the use of SSL certificate verification and encryption.
CVE-2021-23222	A man-in-the-middle attacker can inject false responses to the client's first few queries, despite the use of SSL certificate verification and encryption.
CVE-2021-27212	In OpenLDAP through 2.4.57 and 2.5.x through 2.5.1alpha, an assertion failure in slapd can occur in the issuerAndSignature field of a packet, resulting in a denial of service (daemon exit) via a short timestamp. This is related to schema_init.c and check_signature.c.
CVE-2021-27218	An issue was discovered in GNOME GLib before 2.66.7 and 2.67.x before 2.67.4. If <code>g_byte_array_new_take()</code> was used on a 32-bit platform, the length would be truncated modulo 2^{32} , causing unintended length truncation.
CVE-2021-28153	An issue was discovered in GNOME GLib before 2.66.8. When <code>g_file_replace()</code> is used with <code>G_FILE_CREATE_REPLACE_EXISTING</code> that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceivably be attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly remain unchanged.)
CVE-2021-28165	In Eclipse Jetty 7.2.2 to 9.4.38, 10.0.0.alpha0 to 10.0.1, and 11.0.0.alpha0 to 11.0.1, CPU usage can reach 100% upon startup.
CVE-2021-28831	decompress_gunzip.c in BusyBox through 1.32.1 mishandles the error bit on the huft_build result pointer, with a result in malformed gzip data.
CVE-2021-3200	Buffer overflow vulnerability in libsolvable 2020-12-13 via the Solver * testcase_read(Pool *pool, FILE *fp, const char **resultflagsp) function at src/testcase.c: line 2334, which could cause a denial of service
CVE-2021-32028	A flaw was found in postgresql. Using an INSERT ... ON CONFLICT ... DO UPDATE command on a purpose-crafted table, an attacker could read arbitrary bytes of server memory. The highest threat from this vulnerability is to data confidentiality.
CVE-2021-32029	A flaw was found in postgresql. Using an UPDATE ... RETURNING command on a purpose-crafted table, an attacker could read arbitrary bytes of server memory. The highest threat from this vulnerability is to data confidentiality.
CVE-2021-33061	Insufficient control flow management for the Intel(R) 82599 Ethernet Controllers and Adapters may allow an unauthorized user to access network service via local access.
CVE-2021-33560	Libgcrypt before 1.8.8 and 1.9.x before 1.9.3 mishandles ElGamal encryption because it lacks exponent blinding to protect the mpi_powm, and the window size is not chosen appropriately. This, for example, affects use of ElGamal in OpenPGP.
CVE-2021-33574	The mq_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use the freed memory through its struct sigevent parameter after it has been freed by the caller, leading to a denial of service (application crash).
CVE-2021-33621	The cgi gem before 0.1.0.2, 0.2.x before 0.2.2, and 0.3.x before 0.3.5 for Ruby allows HTTP response splitting. The user input either to generate an HTTP response or to create a CGI::Cookie object.
CVE-2021-33631	Integer Overflow or Wraparound vulnerability in openEuler kernel on Linux (filesystem modules) allows Forced Invalidation of kernel: from 4.19.90 before 4.19.90-2401.3, from 5.10.0-60.18.0 before 5.10.0-183.0.0.
CVE-2021-33928	Buffer overflow vulnerability in function pool_installable in src/repo.h in libsolvable before 0.7.17 allows attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code.

CVE-2021-33929	Buffer overflow vulnerability in function pool_disabled_solvable in src/repo.h in libsolv before 0.7.17 allows attackers to cause a denial of service (crash) or execute arbitrary code.
CVE-2021-33930	Buffer overflow vulnerability in function pool_installable_whatprovides in src/repo.h in libsolv before 0.7.17 allows attackers to cause a denial of service (crash) or execute arbitrary code.
CVE-2021-33938	Buffer overflow vulnerability in function prune_to_recommended in src/policy.c in libsolv before 0.7.17 allows attackers to cause a denial of service (crash) or execute arbitrary code.
CVE-2021-3421	A flaw was found in the RPM package in the read functionality. This flaw allows an attacker who can convince a vulnerable RPM repository, to cause RPM database corruption. The highest threat from this vulnerability is to data confidentiality, integrity, and availability.
CVE-2021-3516	There's a flaw in libxml2's xmllint in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed could trigger a use-after-free. The greatest impact of this flaw is to confidentiality, integrity, and availability.
CVE-2021-3517	There is a flaw in the xml entity encoding functionality of libxml2 in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by an application linked with the affected functionality of libxml2 could trigger an out-of-bounds read. The most likely impact of this flaw is to availability, with some potential impact to confidentiality and integrity if an attacker is able to use memory information.
CVE-2021-3518	There's a flaw in libxml2 in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed could trigger a use-after-free. The greatest impact from this flaw is to confidentiality, integrity, and availability.
CVE-2021-3520	There's a flaw in lz4. An attacker who submits a crafted file to an application linked with lz4 may be able to trigger a memmove() on a negative size argument, causing an out-of-bounds write and/or a crash. The greatest impact of this flaw is to confidentiality and integrity as well.
CVE-2021-3521	There is a flaw in RPM's signature functionality. OpenPGP subkeys are associated with a primary key via a "binding" signature of subkeys prior to importing them. If an attacker is able to add or socially engineer another party's public key, RPM could wrongly trust a malicious signature. The greatest impact of this flaw is to data integrity. To exploit this flaw, an attacker could compromise an RPM repository or convince an administrator to install an untrusted RPM or public key. It is strong recommendation to remove public keys from trusted sources.
CVE-2021-3537	A vulnerability found in libxml2 in versions before 2.9.11 shows that it did not propagate errors while parsing XML documents. If an untrusted XML document was parsed in recovery mode and post-validated, the flaw could be used to cause a denial of service. The greatest impact from this vulnerability is to system availability.
CVE-2021-3541	A flaw was found in libxml2. Exponential entity expansion attack its possible bypassing all existing protection mechanisms. The greatest impact from this vulnerability is to system availability.
CVE-2021-35937	A race condition vulnerability was found in rpm. A local unprivileged user could use this flaw to bypass the checks for CVE-2017-7500 and CVE-2017-7501, potentially gaining root privileges. The highest threat from this vulnerability is to data confidentiality, integrity, and availability as well as system availability.
CVE-2021-35938	A symbolic link issue was found in rpm. It occurs when rpm sets the desired permissions and credentials after installing a package. An attacker could use this flaw to exchange the original file with a symbolic link to a security-critical file and escalate their privileges. The greatest impact from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-35939	It was found that the fix for CVE-2017-7500 and CVE-2017-7501 was incomplete: the check was only implemented for files. A local unprivileged user who owns another ancestor directory could potentially use this flaw to gain root privileges. The greatest impact from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-3601	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn. The trusted CA store should not contain anything that the user does not trust. See github.com/openssl/openssl/issues/5236#issuecomment-119646061
CVE-2021-36222	ec_verify in kdc/kdc_preauth_ec.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.18.1 allows attackers to cause a NULL pointer dereference and daemon crash. This occurs because a return value is not properly checked.
CVE-2021-3669	A flaw was found in the Linux kernel. Measuring usage of the shared memory does not scale with large shared memory. This could lead to resource exhaustion and DoS.
CVE-2021-3671	A null pointer de-reference was found in the way samba kerberos server handled missing sname in TGS-REQ (Ticket Granting Service Request). An authenticated user could use this flaw to crash the samba server.
CVE-2021-37322	GCC c++filt v2.26 was discovered to contain a use-after-free vulnerability via the component cplus-dem.c.
CVE-2021-37600	An integer overflow in util-linux through 2.37.1 can potentially cause a buffer overflow if an attacker were able to write a large number in the /proc/sysvipc/sem file.  Note: This is unexploitable in GNU C Library environments, and possibly in all realistic environments.
CVE-2021-3800	A flaw was found in glib before version 2.63.6. Due to random charset alias, pkexec can leak content from files owned by other users under the right condition.
CVE-2021-38185	GNU cpio through 2.13 allows attackers to execute arbitrary code via a crafted pattern file, because of a dstring.c double-free or out-of-bounds heap write. NOTE: it is unclear whether there are common cases where the pattern file, associated with the pattern file, is used.

CVE-2021-3847	An unauthorized access to the execution of the setuid file with capabilities flaw in the Linux kernel OverlayFS subsystem allows a local capable file from a nosuid mount into another mount. A local user could use this flaw to escalate their privileges on the system.
CVE-2021-39686	In several functions of binder.c, there is a possible way to represent the wrong domain to SELinux due to a race condition. A local privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: Android Version: A-200688826References: Upstream kernel
CVE-2021-4023	A flaw was found in the io-workqueue implementation in the Linux kernel versions prior to 5.15-rc1. The kernel can be tricked into operation triggers the submission of new io-uring operations during a shortage of free space. This flaw allows a local user to submit requests to possibly crash the system.
CVE-2021-40528	The ElGamal implementation in Libgcrypt before 1.9.4 allows plaintext recovery because, during interaction between sender and receiver, a dangerous combination of the prime defined by the receiver's public key, the generator defined by the receiver's private key, and exponents can lead to a cross-configuration attack against OpenPGP.
CVE-2021-4149	A vulnerability was found in btrfs_alloc_tree_b in fs/btrfs/extent-tree.c in the Linux kernel due to an improper lock. A local privilege may cause a denial of service (DOS) due to a deadlock problem.
CVE-2021-4204	An out-of-bounds (OOB) memory access flaw was found in the Linux kernel's eBPF due to an Improper Input Validation. A local user can use a special privilege to crash the system or leak internal information.
CVE-2021-42374	An out-of-bounds heap read in Busybox's unlzma applet leads to information leak and denial of service when crafted input is provided. This can be triggered by any applet/format that
CVE-2021-42376	A NULL pointer dereference in Busybox's hush applet leads to denial of service when processing a crafted shell command. The delimiter character. This may be used for DoS under very rare conditions of filtered command input.
CVE-2021-42378	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted input.
CVE-2021-42379	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted input.
CVE-2021-42380	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted input.
CVE-2021-42381	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted input.
CVE-2021-42382	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted input.
CVE-2021-42384	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted input.
CVE-2021-42385	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted input.
CVE-2021-42386	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted input.
CVE-2021-42574	<p>An issue was discovered in the Bidirectional Algorithm in the Unicode Specification through 14.0. It permits the visual ordering of sequences, which can be used to craft source code that renders different logic than the logical ordering of tokens in the source code. Adversaries can leverage this to encode source code for compilers accepting Unicode such that targeted vulnerabilities are not visible to reviewers.</p> <p> Note: The Unicode Consortium offers the following alternative approach to presenting this concern. An adversary could craft source code that can affect applications that implement support for The Unicode Standard and the Unicode Bidirectional Algorithm. To text display behavior when text includes left-to-right and right-to-left characters, the visual order of tokens in the source code is not the same as the logical order. Additionally, control characters needed to fully support the requirements of bidirectional text can be used to craft source code. Unless mitigated, an adversary could craft source code such that the ordering of tokens perceived by humans is different from the logical order. The Unicode Consortium has documented this class of vulnerability in Unicode Technical Report #36, Unicode Security Considerations. The Unicode Consortium also provides guidance on mitigating this issue in Unicode Technical Standard #39, Unicode Security Mechanisms, and in Unicode Standard Annex #31, Unicode Security. The Unicode Specification allows applications to tailor the implementation in ways that can mitigate misleading visual representations. See Unicode Standard Annex #9, Unicode Bidirectional Algorithm.</p>
CVE-2021-43519	Stack overflow in lua_resume of ldo.c in Lua Interpreter 5.1.0-5.4.4 allows attackers to perform a Denial of Service.
CVE-2021-43618	GNU Multiple Precision Arithmetic Library (GMP) through 6.2.1 has an mpz/inp_raw.c integer overflow and results in a segmentation fault on 32-bit platforms.
CVE-2021-43797	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high-performance network servers. Netty prior to version 4.1.71.Final skips control chars when they are present at the beginning / end of the header name. This is not allowed by the spec and could lead to HTTP request smuggling. Failing to do the validation might cause netty to "send" data to another remote system when used as proxy. This remote system can't see the invalid usage anymore, and therefore the proxy should upgrade to version 4.1.71.Final.
CVE-2021-44568	Two heap-overflow vulnerabilities exist in openSUSE/libsolv libsolv through 13 Dec 2020 in the decisionmap variant. The first is in src/solver.c (line 1940 & line 1995), which could cause a remote Denial of Service.

66

CVE-2022-0536	Improper Removal of Sensitive Information Before Storage or Transfer in NPM follow-redirects prior to 1.14.8.
CVE-2022-1205	A NULL pointer dereference flaw was found in the Linux kernel, Ås Amateur Radio AX.25 protocol functionality. This flaw allows a local user to crash the system.
CVE-2022-1271	An arbitrary file write vulnerability was found in GNU gzip's zgrep utility. When zgrep is applied on the attacker's name), this can overwrite an attacker's content to an arbitrary attacker-selected file. This flaw occurs due to insufficiency with two or more newlines where selected content and the target file names are embedded in crafted multi-line file. This allows a privileged attacker to force zgrep to write arbitrary files on the system.
CVE-2022-1586	An out-of-bounds read vulnerability was discovered in the PCRE2 library in the compile_xclass_matchingpath() function. It involves a unicode property matching issue in JIT-compiled regular expressions. The issue occurs because the character class is not properly handled within JIT.
CVE-2022-1587	An out-of-bounds read vulnerability was discovered in the PCRE2 library in the get_recurse_data_length() function. It affects recursions in JIT-compiled regular expressions caused by duplicate data transfers.
CVE-2022-1664	Dpkg::Source::Archive in dpkg, the Debian package management system, before version 1.21.8, 1.20.10, 1.19.8, 1.19.2, and 1.19.1 has a vulnerability. When extracting untrusted source packages in v2 and v3 source package formats that include a debian directory traversal situations on specially crafted orig.tar and debian.tar tarballs.
CVE-2022-2196	A regression exists in the Linux Kernel within KVM: nVMX that allowed for speculative execution attacks. After L2 cache flush, L1 thinking it doesn't need retpolines or IBPB after running L2 due to KVM (L0) advertising eIBRS support to L2. This allows an attacker to execute code on an indirect branch on the host machine. We recommend upgrading to Kernel 6.2 or past commit 7b1e1e1.
CVE-2022-23476	Nokogiri is an open source XML and HTML library for the Ruby programming language. Nokogiri 1.13.8 and 1.13.7 have a vulnerability in the method Nokogiri::XML::Reader#attribute_hash. This can lead to a null pointer exception. For applications using Nokogiri::XML::Reader to parse untrusted inputs, this may potentially be a vector for a denial of service. For applications using Nokogiri 1.13.10 or later, this vulnerability is not present. Users may be able to search their code for calls to either Nokogiri::XML::Reader#attributes or Nokogiri::XML::Reader#attribute_hash. They are affected.
CVE-2022-23491	Certi is a curated collection of Root Certificates for validating the trustworthiness of SSL certificates while verifying the chain of certificates. 2022.12.07 removes root certificates from "TrustCor" from the root store. These are in the process of being removed. These root certificates are being removed pursuant to an investigation prompted by media reporting that TrustCor's owner is involved in spyware. Conclusions of Mozilla's investigation can be found in the linked google group discussion.
CVE-2022-24823	Netty is an open-source, asynchronous event-driven network application framework. The package io.netty:netty-codec-http contains an insufficient fix for CVE-2021-21290. When Netty's multipart decoders are used local information disclosure is possible if temporary directory if temporary storing uploads on the disk is enabled. This only impacts applications running on Linux. The vulnerability impacts code running on Unix-like systems, and very old versions of Mac OSX and Windows as they share the same code. Version 4.1.77.Final contains a patch for this vulnerability. As a workaround, specify one's own DefaultHttpDataFactory.setBaseDir(...) to set the directory to something that is only readable by the current user.
CVE-2022-2509	A vulnerability found in gnutls. This security flaw happens because of a double free error occurs during verification function.
CVE-2022-25265	In the Linux kernel through 5.16.10, certain binary files may have the exec-all attribute if they were built in approximately 2020 (before kernel 2.4.20). This can cause execution of bytes located in supposedly non-executable regions of a file.
CVE-2022-25313	In Expat (aka libexpat) before 2.4.5, an attacker can trigger stack exhaustion in build_model via a large nesting depth.
CVE-2022-2625	A vulnerability was found in PostgreSQL. This attack requires permission to create non-temporary objects in at least one schema, an administrator to create or update an affected extension in that schema, and the ability to lure or wait for a victim. The attack uses REPLACE or CREATE IF NOT EXISTS. Given all three prerequisites, this flaw allows an attacker to run arbitrary SQL as superuser.
CVE-2022-27672	When SMT is enabled, certain AMD processors may speculatively execute instructions using a target from the sibling cache, potentially resulting in information disclosure.
CVE-2022-27774	An insufficiently protected credentials vulnerability exists in curl 4.9 to and include curl 7.82.0 are affected that could occur when follows HTTP(S) redirects is used with authentication could leak credentials to other services that exist on different domains.
CVE-2022-27776	A insufficiently protected credentials vulnerability in fixed in curl 7.83.0 might leak authentication or cookie headers to another port number.
CVE-2022-27778	A use of incorrectly resolved name vulnerability fixed in 7.83.1 might remove the wrong file when --no-clobber is used.
CVE-2022-27779	libcurl wrongly allows cookies to be set for Top Level Domains (TLDs) if the host name is provided with a trailing slash. curl's "cookie engine" can be rebuilt with or without [Public Suffix List](https://publicsuffix.org/awareness). A rudimentary check exists to at least prevent cookies from being set on TLDs. This check was broken if the host name was not a TLD, allowing arbitrary sites to set cookies that then would get sent to a different and unrelated site or domain.
CVE-2022-27780	The curl URL parser wrongly accepts percent-encoded URL separators like %2F when decoding the host name part of a URL. This can cause a wrong host name when it is later retrieved. For example, a URL like http://example.com/%2F127.0.0.1/, would be decoded as http://example.com/127.0.0.1/. This flaw can be used to circumvent filters, checks and more.

CVE-2022-27781	libcurl provides the `CURLOPT_CERTINFO` option to allow applications to request details to be returned about a function, a malicious server could make libcurl built with NSS get stuck in a never-ending busy-loop when trying to
CVE-2022-27782	libcurl would reuse a previously created connection even when a TLS or SSH related option had been changed that previously used connections in a connection pool for subsequent transfers to reuse if one of them matches the setup left out from the configuration match checks, making them match too easily.
CVE-2022-28321	The Linux-PAM package before 1.5.2-6.1 for openSUSE Tumbleweed allows authentication bypass for SSH login. It correctly restrict login if a user tries to connect from an IP address that is not resolvable via DNS. In such conditions, it still gets access. NOTE: the relevance of this issue is largely limited to openSUSE Tumbleweed and openSUSE Factory.
CVE-2022-28391	BusyBox through 1.35.0 allows remote attackers to execute arbitrary code if netstat is used to print a DNS PTR record. Alternatively, the attacker could choose to change the terminal's colors.
CVE-2022-28948	An issue in the Unmarshal function in Go-Yaml v3 causes the program to crash when attempting to deserialize invalid YAML.
CVE-2022-29155	In OpenLDAP 2.x before 2.5.12 and 2.6.x before 2.6.2, a SQL injection vulnerability exists in the experimental backend within an LDAP query. This can occur during an LDAP search operation when the search filter is processed, due to
CVE-2022-29824	In libxml2 before 2.9.14, several buffer handling functions in buf.c (xmlBuf*) and tree.c (xmlBuffer*) don't check for out-of-bounds memory writes. Exploitation requires a victim to open a crafted, multi-gigabyte XML file. Other software, for example libxslt through 1.1.35, is affected as well.
CVE-2022-30115	Using its HSTS support, curl can be instructed to use HTTPS directly instead of using an insecure clear-text HTTP. This mechanism could be bypassed if the host name in the given URL used a trailing dot while not using one when around - by having the trailing dot in the HSTS cache and *not* using the trailing dot in the URL.
CVE-2022-30115	Using its HSTS support, curl can be instructed to use HTTPS directly instead of using an insecure clear-text HTTP. This mechanism could be bypassed if the host name in the given URL used a trailing dot while not using one when around - by having the trailing dot in the HSTS cache and *not* using the trailing dot in the URL.
CVE-2022-3108	An issue was discovered in the Linux kernel through 5.16-rc6. kfd_parse_subtype_iolink in drivers/gpu/drm/amd/kfd/kfd_ioctl.c will cause the null pointer dereference.
CVE-2022-3114	An issue was discovered in the Linux kernel through 5.16-rc6. imx_register_uart_clocks in drivers/clk/imx/clk.c will cause the null pointer dereference.
CVE-2022-31159	The AWS SDK for Java enables Java developers to work with Amazon Web Services. A partial-path traversal issue exists in the method in the AWS S3 TransferManager component of the AWS SDK for Java v1 prior to version 1.12.261. Applying the `destinationDirectory` argument, but S3 object keys are determined by the application that uploaded the objects. This allows the caller to pass a filesystem object in the object key but contained an issue in the validation logic for the key could bypass the validation logic by including a UNIX double-dot in the bucket key. Under certain conditions, this directory from their S3 bucket that is one level up in the filesystem from their working directory. This issue, if the name prefix matches the destinationDirectory. E.g. for destination directory `/tmp/foo`, the actor can cause a download of a file named `bar`. If `com.amazonaws.services.s3.transfer.TransferManager::downloadDirectory` is used to download an untrusted file, that bucket can be written outside of the intended destination directory. Version 1.12.261 contains a patch for this issue. To reproduce, pass a `com.amazonaws.services.s3.transfer.TransferManager::downloadDirectory`, pass a `KeyFilter` that forbids `S3Object` return a string containing the substring `../`.
CVE-2022-3116	The Heimdal Software Kerberos 5 implementation is vulnerable to a null pointer dereference. An attacker with network access to the vulnerable code path can cause the application to crash.
CVE-2022-31197	PostgreSQL JDBC Driver (PgJDBC for short) allows Java programs to connect to a PostgreSQL database using standard JDBC. The PGJDBC implementation of the `java.sql.ResultSet.refreshRow()` method is not performing escaping of column names. If a column name contains a statement terminator, e.g. `;`, could lead to SQL injection. This could lead to executing additional SQL code. User applications that do not invoke the `ResultSet.refreshRow()` method are not impacted. User application that does invoke the method and the underlying database that they are querying via their JDBC application may be under the control of an attacker. The application can then execute SQL against a table name whose column names would contain the malicious SQL and subsequently return a `ResultSet`. Note that the application's JDBC user and the schema owner need not be the same. A JDBC application that uses a database schema owned by potentially malicious less-privileged users would be vulnerable. In that situation it may be possible to cause the application to execute commands as the privileged user. Patched versions will be released as soon as possible. There are no known workarounds for this issue.
CVE-2022-32208	When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly. This flaw allows an attacker to go unnoticed and even allows it to inject data to the client.

CVE-2022-3358	OpenSSL supports creating a custom cipher via the legacy <code>EVP_CIPHER_meth_new()</code> function and associated functions in OpenSSL 3.0 and application authors are instead encouraged to use the new provider mechanism in order to improve security. Versions 3.0.0 to 3.0.5 incorrectly handle legacy custom ciphers passed to the <code>EVP_EncryptInit_ex2()</code> , <code>EVP_DecryptInit_ex2()</code> (as well as other similarly named encryption and decryption initialisation functions). Instead of using the custom cipher, an equivalent cipher from the available providers. An equivalent cipher is found based on the NID passed to <code>EVP_CIPHER_meth_new()</code> , supposed to represent the unique NID for a given cipher. However it is possible for an application to incorrectly pass a NID to <code>EVP_CIPHER_meth_new()</code> . When <code>NID_undef</code> is used in this way the OpenSSL encryption/decryption initialisation functions will be equivalent and will fetch this from the available providers. This will succeed if the default provider has been loaded that offers this cipher). Using the <code>NULL</code> cipher means that the plaintext is emitted as the ciphertext. Applications should call <code>EVP_CIPHER_meth_new()</code> using <code>NID_undef</code> and subsequently use it in a call to an encryption/decryption initialisation function. SSL/TLS are not impacted by this issue. Fixed in OpenSSL 3.0.6 (Affected 3.0.0-3.0.5).
CVE-2022-3437	A heap-based buffer overflow vulnerability was found in Samba within the GSSAPI <code>unwrap_des()</code> and <code>unwrap_des3()</code> routines. Triple-DES decryption routines in the Heimdal GSSAPI library allow a length-limited write buffer overflow on memory. An attacker could send a maliciously small packet. This flaw allows a remote user to send specially crafted malicious data to the application, potentially leading to a Denial of Service (DoS) attack.
CVE-2022-34903	GnuPG through 2.3.6, in unusual situations where an attacker possesses any secret-key information from a victim's GPGME (e.g., via a GPGME) are met, allows signature forgery via injection into the status line.
CVE-2022-3515	A vulnerability was found in the Libksba library due to an integer overflow within the CRL parser. The vulnerability allows a remote attacker to execute arbitrary code or cause a denial of service (DoS) on the target system by passing specially crafted data to the application, for example, a malicious S/MIME message.
CVE-2022-35252	When curl is used to retrieve and parse cookies from a HTTP(S) server, it accepts cookies using control codes that might make the server return 400 responses. Effectively allowing a "sister site" to deny service to all siblings.
CVE-2022-3566	A vulnerability, which was classified as problematic, was found in Linux Kernel. This affects the function <code>tcp_get_syncookie</code> in the TCP Handler. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. The identifier of the vulnerability is CVE-2022-3566.
CVE-2022-3567	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function <code>ip6_route_output</code> in the IPv6 Handler. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. The identifier of the vulnerability is CVE-2022-3567.
CVE-2022-36944	Scala 2.13.x before 2.13.9 has a Java deserialization chain in its JAR file. On its own, it cannot be exploited. There is no known exploit for this vulnerability. In such situations, it allows attackers to erase contents of arbitrary files or execute arbitrary code (specifically, <code>Function0</code> functions) via a gadget chain.
CVE-2022-3707	A double-free memory flaw was found in the Linux kernel. The Intel GVT-g graphics driver triggers VGA card system errors when <code>intel_gvt_dma_map_guest_page</code> function. This issue could allow a local user to crash the system.
CVE-2022-37434	zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in <code>inflate</code> in <code>inflate.c</code> via a large gzip header. Applications that call <code>inflateGetHeader</code> are affected. Some common applications bundle the affected zlib source code but may be unaffected if they use a system-installed version (e.g., <code>nodejs/node</code> reference).
CVE-2022-40152	Those using Woodstox to parse XML data may be vulnerable to Denial of Service attacks (DOS) if DTD support is enabled. If supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may supply a denial of service.
CVE-2022-40303	An issue was discovered in <code>libxml2</code> before 2.10.3. When parsing a multi-gigabyte XML document with the <code>XML_PARSE_NOBLANKS</code> option, integer counters can overflow. This results in an attempt to access an array at a negative 2GB offset, typically leading to a crash.
CVE-2022-40304	An issue was discovered in <code>libxml2</code> before 2.10.3. Certain invalid XML entity definitions can corrupt a hash table leading to memory errors. In one case, a double-free can be provoked.
CVE-2022-4129	A flaw was found in the Linux kernel's Layer 2 Tunneling Protocol (L2TP). A missing lock when clearing <code>sk_user_data</code> leads to a pointer dereference. A local user could use this flaw to potentially crash the system causing a denial of service.
CVE-2022-41916	Heimdal is an implementation of ASN.1/DER, PKIX, and Kerberos. Versions prior to 7.7.1 are vulnerable to a denial of service (DoS) attack via certificate validation library, affecting the KDC (via <code>PKINIT</code>) and kinit (via <code>PKINIT</code>), as well as any third-party applications. Users should upgrade to Heimdal 7.7.1 or 7.8. There are no known workarounds for this issue.
CVE-2022-42010	An issue was discovered in D-Bus before 1.12.24, 1.13.x before 1.14.4, and 1.15.x before 1.15.2. An attacker could use this flaw to crash and other programs that use <code>libdbus</code> to crash when receiving a message with certain invalid type signatures.
CVE-2022-42011	An issue was discovered in D-Bus before 1.12.24, 1.13.x before 1.14.4, and 1.15.x before 1.15.2. An attacker could use this flaw to crash and other programs that use <code>libdbus</code> to crash when receiving a message where an array length is inconsistent with the type signature.
CVE-2022-42012	An issue was discovered in D-Bus before 1.12.24, 1.13.x before 1.14.4, and 1.15.x before 1.15.2. An attacker could use this flaw to crash and other programs that use <code>libdbus</code> to crash by sending a message with attached file descriptors in an unexpected format.
CVE-2022-4285	An illegal memory access flaw was found in the <code>binutils</code> package. Parsing an ELF file containing corrupt symbol version information could lead to a denial of service. This issue is the result of an incomplete fix for CVE-2020-16599.

CVE-2022-42898	PAC parsing in MIT Kerberos 5 (aka krb5) before 1.19.4 and 1.20.x before 1.20.1 has integer overflows that may lead to a crash in kadmind, or a GSS or Kerberos application server) on 32-bit platforms (which have a resultant heap-based buffer overflow) on other platforms. This occurs in krb5_pac_parse in lib/krb5/krb/pac.c. Heimdal before 7.7.1 has "a similar bug."
CVE-2022-43680	In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCtxt situations.
CVE-2022-4379	A use-after-free vulnerability was found in __nfs42_ssc_open() in fs/nfs/nfs4file.c in the Linux kernel. This flaw allows an attacker to cause a kernel crash.
CVE-2022-4382	A use-after-free flaw caused by a race among the superblock operations in the gadgetfs Linux driver was found. It occurs when the driver that is running the gadgetfs side.
CVE-2022-44640	Heimdal before 7.7.1 allows remote attackers to execute arbitrary code because of an invalid free in the ASN.1 code (KDC).
CVE-2022-45142	The fix for CVE-2022-3437 included changing memcmp to be constant time and a workaround for a compiler bug in memcmp. When these patches were backported to the heimdal-7.7.1 and heimdal-7.8.0 branches (and possibly others), causing the validation of message integrity codes in gssapi/arcfour to be inverted.
CVE-2022-45868	The web-based admin console in H2 Database Engine before 2.2.220 can be started via the CLI with the argument --web-console to allow a user to specify the password in cleartext for the web admin console. Consequently, a local user (or an attacker that has access to the command line) means) would be able to discover the password by listing processes and their arguments. NOTE: the vendor states that passwords should never be passed on the command line and every qualified DBA or system administrator is expected to know this. Fixed in 2.2.220.
CVE-2022-45873	systemd 250 and 251 allows local users to achieve a systemd-coredump deadlock by triggering a crash that has a local user in shared/elf-util.c. The exploitation methodology is to crash a binary calling the same function recursively, and push the backtrace large enough to cause the deadlock. This must be done 16 times when MaxConnections=16 is set for the service.
CVE-2022-45886	An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_net.c has a .disconnect verb that leads to a use-after-free.
CVE-2022-45887	An issue was discovered in the Linux kernel through 6.0.9. drivers/media/usb/ttusb-dec/ttusb_dec.c has a memory leak in dvb_frontend_detach call.
CVE-2022-45919	An issue was discovered in the Linux kernel through 6.0.10. In drivers/media/dvb-core/dvb_ca_en50221.c, a use-after-free occurs after an open, because of the lack of a wait_event.
CVE-2022-47629	Libksba before 1.6.3 is prone to an integer overflow vulnerability in the CRL signature parser.
CVE-2022-48174	There is a stack overflow vulnerability in ash.c:6030 in busybox before 1.35. In the environment of Internet of Vehicles, an attacker can execute arbitrary code to arbitrary code execution.
CVE-2022-48554	File before 5.43 has an stack-based buffer over-read in file_copystr in funcs.c. NOTE: "File" is the name of an OpenSSH file.
CVE-2022-48566	An issue was discovered in compare_digest in Lib/hmac.py in Python through 3.9.1. Constant-time-defeating optimization in hmac.compare_digest.
CVE-2022-48566	An issue was discovered in compare_digest in Lib/hmac.py in Python through 3.9.1. Constant-time-defeating optimization in hmac.compare_digest.
CVE-2022-48626	In the Linux kernel, the following vulnerability has been resolved: moxart: fix potential use-after-free on remove path. The structure could be accessed after it was freed in moxart_remove(), so fix this by saving the base register of the device before dereference.
CVE-2022-48645	In the Linux kernel, the following vulnerability has been resolved: net: enetc: deny offload of tc-based TSN features. ENETC (taprio, cbs, gate, police) are configured through a mix of command BD ring messages and port registers. The registers are a region of the ENETC memory map which are only accessible from the PCIe Physical Function. The current implementation allows access to these registers from the user space. Moreover, attempting to access these registers crashes the kernel: \$ echo 1 > /sys/bus/pci/devices/0000:00:02:00/enetc_vf [1957:ef00] type 00 class 0x020001 fsl_enetc_vf 0000:00:01.0: Adding to iommu group 15 fsl_enetc_vf 0000:00:01.0: fsl_enetc_vf 0000:00:01.0 eno0vf0: renamed from eth0 \$ tc qdisc replace dev eno0vf0 root taprio num_tc 8 map 0 1@4 1@5 1@6 1@7 base-time 0 \ sched-entry S 0x7f 900000 sched-entry S 0x80 100000 flags 0x2 Unable to handle kernel NULL pointer dereference at 0000000000000000. Internal error: Oops: 96000007 [#1] PREEMPT SMP pc : enetc_setup_tc_taprio+0x170/0x47c 1 Call trace: enetc_setup_tc_taprio+0x170/0x47c enetc_setup_tc+0x38/0x2dc taprio_change+0x43c/0x970 taprio_inetdev_init+0x10/0x10 tc_modify_qdisc+0x1fc/0x6c0 rtnetlink_rcv_msg+0x12c/0x390 Split enetc_setup_tc() into separate functions for taprio and qdisc. enetc_qos.o from being included into enetc-vf.ko, since it serves absolutely no purpose there.
CVE-2022-48655	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Harden accesses to the reset descriptors by the index upon the SCMI drivers requests through the SCMI reset operations interface can potentially lead to a driver misbehave. Add an internal consistency check before any such domains descriptors accesses.

CVE-2022-48666	<p>In the Linux kernel, the following vulnerability has been resolved: scsi: core: Fix a use-after-free There are two .exit implementations. Both implementations use resources associated with the SCSI host. Make sure that these resources are freed when .exit_cmd_priv is called by waiting inside scsi_remove_host() until the tag set has been freed. This commit fixes the use-after-free bug.</p> <pre>BUG: KASAN: use-after-free in scsi_remove_host+0x27/0xd0 [ib_srp] Read of size 8 at addr ffff888100337000 by task multipathd/16727 Call Trace: <TASK> dump_stack+0x5e/0x5db kasan_report+0xab/0x120 srp_exit_cmd_priv+0x27/0xd0 [ib_srp] scsi_mq_exit_request+0x4d/0x70 blk_mq_free_map_and_rqs+0x6e/0x100 blk_mq_free_tag_set+0x2b/0x160 scsi_host_dev_release+0xf3/0x1a0 scsi_device_release+0xa5/0x120 device_release+0x54/0xe0 kobject_put+0xa5/0x120 scsi_device_dev_release_usercontext+0x4c1/0x50 device_release+0x54/0xe0 kobject_put+0xa5/0x120 scsi_disk_release+0x3f/0x50 device_release+0x54/0xe0 kobject_put+0x17f/0x1b0 device_release+0x54/0xe0 kobject_put+0xa5/0x120 dm_put_table_device+0xa3/0x160 [dm_mod] dm_free_priority_group+0xd8/0x110 [dm_multipath] free_multipath+0x94/0xe0 [dm_multipath] dm_table_destroy+0x196/0x350 [dm_mod] dev_remove+0x10c/0x160 [dm_mod] ctl_ioctl+0x2c2/0x590 [dm_mod] dm_ctl_ioctl+0x10b/0x160 [dm_mod] dm_ctl_ioctl+0x5/0x10 [dm_mod] __x64_sys_ioctl+0xb4/0xf0 do_syscall_64+0x3b/0x90 entry_SYSCALL_64+0x0/0xffffffff</pre>
CVE-2022-48674	<p>In the Linux kernel, the following vulnerability has been resolved: erofs: fix pcluster use-after-free on UP platforms disabled, KASAN reports as below: ===== free in __mutex_lock+0xe5/0xc30 Read of size 8 at addr ffff8881094223f8 by task stress/7789 CPU: 0 PID: 7789 g0d53d2e882f9 #3 Hardware name: Red Hat KVM, BIOS 0.5.1 01/01/2011 Call Trace: <TASK> .. __mutex_lock+0x8ce/0x1560 .. z_erofs_readahead+0x31c/0x580 .. Freed by task 7787 kasan_save_stack+0x1e/0x40 kasan_set_track+0x20/0x40 __kasan_slab_free+0x10c/0x190 kmem_cache_free+0xed/0x380 rcu_core+0x3d5/0xc90 __do_softirq+0x10/0x10 creation: kasan_save_stack+0x1e/0x40 __kasan_record_aux_stack+0x97/0xb0 call_rcu+0x3d/0x3f0 erofs_shrink_slab+0xdc/0x170 shrink_slab.constprop.0+0x296/0x530 drop_slab+0x1c/0x70 drop_caches_sysctl_handler+0x70/0x80 vfs_write+0x555/0x6c0 ksys_write+0xbe/0x160 do_syscall_64+0x3b/0x90 The root cause is that erofs_workgroup_it causes a race that the pcluster reuses unexpectedly before freeing. Since UP platforms are quite rare now, such path is specific-designed path directly instead.</p>
CVE-2022-48708	<p>In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix potential NULL dereference pcs_set_mux(). pinmux_generic_get_function() can return NULL and the pointer "function" was dereferenced with Verification Center (linuxtesting.org) with SVACE.</p>
CVE-2022-48781	<p>In the Linux kernel, the following vulnerability has been resolved: crypto: af_alg - get rid of alg_memory_allocated not seem to be really used. alg_proto does have a .memory_allocated field, but no corresponding .sysctl_mem. This is true, but all sk_prot_mem_limits() users will trigger a NULL dereference [1]. This was not a problem until SO_REUSEADDR protection fault, probably for non-canonical address 0xdffffc0000000001: 0000 [#1] PREEMPT SMP KASAN KASAN: null-dereference in sk_prot_mem_limits+0x0/0x10 CPU: 1 PID: 3591 Comm: syz-executor153 Not tainted 5.17.0-rc3-00000000000000000000000000000000 CPU: 1 PID: 3591 Comm: syz-executor153 Not tainted 5.17.0-rc3-00000000000000000000000000000000 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 RIP: 0010:sk_prot_mem_limits+0x0/0x10 [inline] RIP: 0010:sock_reserve_memory+0x1d7/0x330 net/core/sock.c:1000 Code: 08 00 74 08 48 89 ef e8 27 20 c5 08 48 89 e8 48 c1 e8 03 48 b9 00 00 00 00 00 00 ff df <80> 3c 08 00 74 08 48 89 ef e8 fb 1f bb f9 48 8b 6d 00 4 c5 08 48 89 e8 48 c1 e8 03 48 b9 00 00 00 00 00 00 ff df <80> 3c 08 00 74 08 48 89 ef e8 fb 1f bb f9 48 8b 6d 00 4 EFLAGS: 00010202 RAX: 0000000000000001 RBX: ffff88814aabc000 RCX: dffffc0000000000 RDX: 00000000 RDI: ffffffff90e18120 RBP: 0000000000000000 R08: dffffc0000000000 R09: ffffffff21c3025 R10: ffffffff21c3025 R11: 0000000000000000 R12: 0000000000000001 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 0000555556e08300 (0000) GS:ffff8880b9b00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fc74416f130 CR3: 000000000003506e DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR7: 0000000000000040 Call Trace: <TASK> sock_setsockopt+0x14a9/0x3a30 net/core/sock.c:1446 __sys_setsockopt+0x10/0x10 __do_sys_setsockopt net/socket.c:2191 [inline] __se_sys_setsockopt net/socket.c:2188 [inline] __x64_sys_setsockopt do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x44/0xd0 arch/x86/entry/common.c:80 entry_SYSCALL_64+0x0/0xffffffff RIP: 0033:0x7fc7440fdde9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 15 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 d6 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffe98f07968 EFLAGS: 00000000 RAX: ffffffff90e18120 RBX: 0000000000000003 RCX: 00007fc7440fdde9 RDX: 0000000000000049 RSI: 00000000 RBP: 0000000000000000 R08: 0000000000000000 R09: 00007ffe98f07990 R10: 0000000020000000 R11: 00000000 R12: 0000000000000000 R13: 00007ffe98f079a0 R14: 00007ffe98f079e0 R15: 0000000000000000 </TASK> Modules linked in: ---[end trace 0010:sk_prot_mem_limits include/net/sock.h:1523 [inline] RIP: 0010:sock_reserve_memory+0x1d7/0x330 net/core/sock.c:1000 Code: 08 00 74 08 48 89 ef e8 27 20 c5 08 48 89 e8 48 c1 e8 03 48 b9 00 00 00 00 00 00 ff df <80> 3c 08 00 74 08 48 89 ef e8 fb 1f bb f9 48 8b 6d 00 4 c5 08 48 89 e8 48 c1 e8 03 48 b9 00 00 00 00 00 00 ff df <80> 3c 08 00 74 08 48 89 ef e8 fb 1f bb f9 48 8b 6d 00 4 c5 08 48 89 e8 48 c1 e8 03 48 b9 00 00 00 00 00 00 ff df <80> 3c 08 00 74 08 48 89 ef e8 fb 1f bb f9 48 8b 6d 00 4 RSP: 0018:ffff90001f1fb68 EFLAGS: 00010202 RAX: 0000000000000001 RBX: ffff88814aabc000 RCX: dffffc0000000000 RDI: ffffffff90e18120 RBP: 0000000000000000 R08: dffffc0000000000 R09: ffffffff21c3025 R10: 0000000000000000 R11: 0000000000000000 R12: ffffffff8d109840 R13: 0000000000000001 R14: 0000000000000000 R15: 0000555556e08300(0000) GS:ffff8880b9b00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fc74416f130 CR3: 000000000003506e DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR7: 0000000000000040</p>
CVE-2022-48791	<p>In the Linux kernel, the following vulnerability has been resolved: scsi: pm8001: Fix use-after-free for aborted TMF occur if a TMF sas_task is aborted before we handle the IO completion in mpi_ssp_completion(). The abort occurs when SAS_TASK_STATE_ABORTED flag is set and the sas_task is freed in pm8001_exec_internal_tmf_task(). However, the IO completion still thinks that the sas_task is available. Fix this by clearing the ccb->task if the TMF times out - the pointer is cleared.</p>
CVE-2022-48792	<p>In the Linux kernel, the following vulnerability has been resolved: scsi: pm8001: Fix use-after-free for aborted SSI may occur if a sas_task is aborted by the upper layer before we handle the I/O completion in mpi_ssp_completion(). The following are the two steps in handling those I/O completions: - Call complete() to inform the upper layer handler of the completion of the sas_task in pm8001_ccb_task_free() call. When complete() is called, the upper layer handler will touch the associated sas_task afterwards, but we do so in the pm8001_ccb_task_free() call. Fix by swapping the order of the two steps.</p>

CVE-2022-48814	In the Linux kernel, the following vulnerability has been resolved: net: dsa: seville: register the mdiobus under devres ("net: dsa: realtek: register the MDIO bus under devres") 5135e96a3dd2 ("net: dsa: don't allocate the slave_mii_bus when called from devm_mdiobus_free() <- devres_release_all() <- __device_release_driver(), and that mdiobus was used by VSC9959 switch is a platform device, so the initial set of constraints that I thought would cause this (I2C or SPI bus) do not apply. But there is one more which applies here. If the DSA master itself is on a bus that calls ->remove from the fsl-mc bus), there is a device link between the switch and the DSA master, and device_links_unbind_consumer shutdown. So the same treatment must be applied to all DSA switch drivers, which is: either use devres for both the switch and use devres at all. The seville driver has a code structure that could accommodate both the mdiobus_unregister and mdiobus_free dependency upon mscm_miim_setup() from mdio-mscm-miim.c, which calls devm_mdiobus_alloc_size() on its behalf. Instead of exporting yet one more symbol mscm_miim_teardown(), let's work with devres and replace of_mdiobus_register with devres, we can ensure that devres doesn't free a still-registered bus (it either runs both callbacks, or none).
CVE-2022-48816	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: lock against ->sock changing during asynchronous unless ->recv_mutex is held. So it is important to hold that mutex. Otherwise a sysfs read can trigger a race. ("SUNRPC: Check if the xprt is connected before handling sysfs reads") appears to attempt to fix this problem, but it's not clear if it's sufficient.
CVE-2022-48818	In the Linux kernel, the following vulnerability has been resolved: net: dsa: mv88e6xxx: don't use devres for mdiobus ("net: dsa: realtek: register the MDIO bus under devres") 5135e96a3dd2 ("net: dsa: don't allocate the slave_mii_bus when called from devm_mdiobus_free() <- devres_release_all() <- __device_release_driver(), and that mdiobus was used by mv88e6xxx is an MDIO device, so the initial set of constraints that I thought would cause this (I2C or SPI buses) do not apply. But there is one more which applies here. If the DSA master itself is on a bus that calls ->remove from the fsl-mc bus), there is a device link between the switch and the DSA master, and device_links_unbind_consumer shutdown. systemd-shutdown[1]: Powering off. mv88e6085 0x0000000008b96000:00 sw_glo: Link is Down fsl-mc group 7 fsl-mc dpbp.8: Removing from iommu group 7 -----[cut here]----- kernel BUG at drivers/net/phy/bug.h:0 [#1] PREEMPT SMP Modules linked in: CPU: 0 PID: 1 Comm: systemd-shutdown Not tainted 5.16.5-000a00000+0x44/0x50 lr : devm_mdiobus_free+0x10/0x20 Call trace: mdiobus_free+0x44/0x50 devm_mdiobus_free+0x10/0x20 __device_release_driver+0x190/0x220 device_release_driver_internal+0xac/0xb0 device_links_unbind_consumer+0x4c/0x220 device_release_driver_internal+0xac/0xb0 device_links_unbind_consumer+0x4c/0x220 device_release_driver+0x28/0x40 bus_remove_device+0x118/0x124 device_del+0x174/0x420 fsl_mc_device_remove+0xc/0x20 device_for_each_child+0x58/0xa0 dprc_remove+0x90/0xb0 fsl_mc_driver_remove+0x20/0x5c __device_release_driver+0x28/0x40 bus_remove_device+0x118/0x124 device_del+0x174/0x420 fsl_mc_bus_remove+0xc/0x1c platform_shutdown+0x20/0x30 device_shutdown+0x154/0x330 kernel_power_off+0x34/0x6c __do_sys_shutdown+0x20/0x30 invoke_syscall.constprop.0+0x4c/0xe0 do_el0_svc+0x4c/0x150 el0_svc+0x24/0xb0 el0t_64_sync_handler+0x10/0x100 el0t_64_sync+0x10/0x100 So the same treatment must be applied to all DSA switch drivers, which is: either use devres for both the mdiobus and the switch at all. The Marvell driver already has a good structure for mdiobus removal, so just plug in mdiobus_free and get rid of devres.
CVE-2022-48826	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: Fix deadlock on DSI device attach error with host device's lock held. Un-registering host in "device attach" error path (ex: probe retry) will result in deadlock on DSI display. Startup Call trace: [35.043036] rt_mutex_slowlock.constprop.21+0x184/0x1b8 [35.043048] mutex_unlock+0x10/0x18 [35.043052] device_unregister+0x20/0x40 [35.043082] mipi_dsi_remove_device_fn+0x10/0x18 [35.043090] mipi_dsi_host_unregister+0x40/0x90 [35.043115] vc4_dsi_host_attach+0xf0/0x120 [vc4_dsi_host_attach+0x30/0x48 [35.043209] tc358762_probe+0x128/0x164 [tc358762] [35.043225] mipi_dsi_drv_probe+0x28/0x38 [35.043244] __driver_probe_device+0x80/0xe8 [35.043254] driver_probe_device+0xb8/0x118 [35.043263] __device_attach+0x10/0x18 [35.043281] __device_attach+0xf0/0x150 [35.043290] device_initial_probe+0x1c/0x20 [35.043308] deferred_probe_work_func+0xa0/0xe0 [35.043318] process_one_work+0x254/0x700 [35.043339] kthread+0x19c/0x1a8 [35.043348] ret_from_fork+0x10/0x20 Shutdown Call trace: [365.565417] Cpu0: 0x148/0x200 [365.565452] __schedule+0x340/0x9c8 [365.565467] schedule+0x48/0x110 [365.565479] schedu_wait_for_completion+0xac/0x138 [365.565509] __flush_work+0x218/0x4e0 [365.565523] flush_work+0x1c/0x20 [365.565537] __do_sys_shutdown+0x20/0x30 [365.565550] device_shutdown+0x24/0x348 [365.565561] kernel_restart_prepare+0x40/0x50 [365.565571] __do_sys_reboot+0x10c/0x220 [365.565605] __arm64_sys_reboot+0x2c/0x38 [365.565619] invoke_syscall.constprop.3+0xfc/0x120 [365.565648] do_el0_svc+0x2c/0x90 [365.565661] el0_svc+0x4c/0xf0 [365.565675] el0t_64_sync+0x10/0x100 [365.565682] el0t_64_sync+0x180/0x184

CVE-2022-48833	In the Linux kernel, the following vulnerability has been resolved: btrfs: skip reserved bytes warning on unmount a changes made by commit c2e39305299f01 ("btrfs: clear extent buffer uptodate when we fail to write it") and its fol ("btrfs: check WRITE_ERR when trying to read an extent buffer"), we can now end up not cleaning up space reser transaction abort happens, as well as not cleaning up still dirty extent buffers. This happens because if writeback fo have cleared the bit EXTENT_BUFFER_UPTODATE from the extent buffer and we have also set the bit EXTENT when trying to free the log tree with free_log_tree(), which iterates over the tree, we can end up getting an -EIO err read_extent_buffer_pages() returns -EIO if an extent buffer does not have EXTENT_BUFFER_UPTODATE set an bit set. Getting that -EIO means that we return immediately as we can not iterate over the entire tree. In that case w extent buffer in the respective block group and space_info object. When this happens we get the following traces w BTRFS: error (device dm-0) in cleanup_transaction:1913: errno=-5 IO failure [174957.286497] BTRFS: error (dev errno=-5 IO failure [174957.399379] -----[cut here]----- [174957.402497] WARNING: CPU: 2 PID: 3 btrfs_put_block_group+0x77/0xb0 [btrfs] [174957.407523] Modules linked in: btrfs overlay dm_zero (...) [174957 umount Tainted: G W 5.16.0-rc5-btrfs-next-109 #1 [174957.426689] Hardware name: QEMU Standard PC (i440F g155821a1990b-prebuilt.qemu.org 04/01/2014 [174957.428716] RIP: 0010:btrfs_put_block_group+0x77/0xb0 [btr bd (...) [174957.432867] RSP: 0018:ffffb70d41cfff00 EFLAGS: 00010206 [174957.433632] RAX: 000000000000 ffff8b0758edd1c8 [174957.434689] RDX: 0000000000000001 RSI: ffffffff0b467e7 RDI: ffff8b0758edd000 [174 0000000000000000 R09: 0000000000000000 [174957.437114] R10: 0000000000000246 R11: 00000000000000 R13: ffff8b09c3848198 R14: ffff8b0758edd188 R15: dead000000000100 [174957.439317] FS: 0000f328fb82800 knlGS:0000000000000000 [174957.440402] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [174957.441 CR3: 0000000404f4e005 CR4: 000000000370ee0 [174957.442117] DR0: 0000000000000000 DR1: 000000000 [174957.443076] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [174957.443948] C [174957.444538] btrfs_free_block_groups+0x255/0x3c0 [btrfs] [174957.445238] close_ctree+0x301/0x357 [btrfs] +0x16c/0x290 [174957.446250] generic_shutdown_super+0x74/0x120 [174957.446832] kill_anon_super+0x14/0x +0x12/0x20 [btrfs] [174957.447890] deactivate_locked_super+0x31/0xa0 [174957.448440] cleanup_mnt+0x147/0 +0x5c/0xa0 [174957.449336] exit_to_user_mode_prepare+0x1e5/0x1f0 [174957.449934] syscall_exit_to_user_mo do_syscall_64+0x48/0xc0 [174957.450980] entry_SYSCALL_64_after_hwframe+0x44/0xae [174957.451605] RI Code: 03 0c 00 f7 (...) [174957.454320] RSP: 002b:00007fff13564ec8 EFLAGS: 00000246 ORIG_RAX: 0000000 0000000000000000 RBX: 0000f328feca264 RCX: 0000f328fdc4a97 [174957.456131] RDX: 0000000000000000
CVE-2022-48852	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: hdmi: Unregister codec device on unb device but we don't unregister it on unbind, leading to a device leakage. Unregister our device at unbind.
CVE-2022-48859	In the Linux kernel, the following vulnerability has been resolved: net: marvell: presteria: Add missing of_node_put This node pointer is returned by of_find_compatible_node() with refcount incremented. Calling of_node_put() to a
CVE-2022-4886	Ingress-nginx `path` sanitization can be bypassed with `log_format` directive.
CVE-2023-0361	A timing side-channel in the handling of RSA ClientKeyExchange messages was discovered in GnuTLS. This side encrypted in the RSA ciphertext across a network in a Bleichenbacher style attack. To achieve a successful decrypt amount of specially crafted messages to the vulnerable server. By recovering the secret from the ClientKeyExchange, decrypt the application data exchanged over that connection.
CVE-2023-0458	A speculative pointer dereference problem exists in the Linux Kernel on the do_prlimit() function. The resource arg and is used in pointer arithmetic for the 'rlim' variable and can be used to leak the contents. We recommend upgrading commit-739790605705ddcf18f21782b9c99ad7d53a8c11
CVE-2023-0459	Copy_from_user on 64-bit versions of the Linux kernel does not implement the __uaccess_begin_nospec allowing check and pass a kernel pointer to copy_from_user(). This would allow an attacker to leak information. We recommend commit-774e19ef0ff8061ef55957c3abd71614ef0f42f47
CVE-2023-0461	There is a use-after-free vulnerability in the Linux Kernel which can be exploited to achieve local privilege escalation configuration flag CONFIG_TLS-7or CONFIG_XFRM_ESPINTCP-7has to be configured, but the operation doe is a use-after-free bug of icsk_ulp_data-7of a struct inet_connection_sock. When CONFIG_TLS-7is enabled, user (tls_context) on a connected tcp socket. The context is not cleared if this socket is disconnected and reused as a listener, the context is inherited and vulnerable. The setsockopt-7TCP_ULP-7operation does not require any privi commit-72c02d41d71f90a5168391b6a5f2954112ba2307c
CVE-2023-0597	A flaw possibility of memory leak in the Linux kernel cpu_entry_area mapping of X86 CPU data to memory was f exception stack(s) or other important data. A local user could use this flaw to get access to some important data wit
CVE-2023-1073	A memory corruption flaw was found in the Linux kernel, Aô's human interface device (HID) subsystem in how a u allows a local user to crash or potentially escalate their privileges on the system.
CVE-2023-1074	A memory leak flaw was found in the Linux kernel's Stream Control Transmission Protocol. This issue may occur service and someone connects to this service. This could allow a local user to starve resources, causing a denial of
CVE-2023-1075	A flaw was found in the Linux Kernel. The tls_is_tx_ready() incorrectly checks for list emptiness, potentially access leaking the last byte of the confused field that overlaps with rec->tx_ready.
CVE-2023-1078	A flaw was found in the Linux Kernel in RDS (Reliable Datagram Sockets) protocol. The rds_rm_zerocopy_callba causing a type confusion. Local user can trigger this with rds_message_put(). Type confusion leads to `struct rds_n something else that is potentially controlled by local user. It is known how to trigger this, which causes an out of bo

CVE-2023-1079	A flaw was found in the Linux kernel. A use-after-free may be triggered in <code>asus_kbd_backlight_set</code> when plugging which advertises itself as an Asus device. Similarly to the previous known CVE-2023-25012, but in asus devices, the controller while the device is disconnecting, triggering a use-after-free on the struct <code>asus_kbd_leds *led</code> structure. A local attacker can cause memory corruption with controlled data.
CVE-2023-1118	A flaw use after free in the Linux kernel integrated infrared receiver/transceiver driver was found in the way user data is handled. This flaw allows a local attacker to crash the system or potentially escalate their privileges on the system.
CVE-2023-1192	A use-after-free flaw was found in <code>smb2_is_status_io_timeout()</code> in CIFS in the Linux Kernel. After CIFS transfers a local variable points to the memory region, and if the system call frees it faster than CIFS uses it, CIFS will access freed memory.
CVE-2023-1281	Use After Free vulnerability in Linux kernel traffic control index filter (tcindex) allows Privilege Escalation. The vulnerability exists in the <code>tcindex_delete</code> function which does not properly deactivate filters in case of a perfect hashes while deleting the underlaying structure. A local attacker user can use this vulnerability to elevate its privileges to root. This issue affects Linux Kernel: from 4.14 before git commit ee05917.
CVE-2023-1513	A flaw was found in KVM. When calling the <code>KVM_GET_DEBUGREGS</code> ioctl, on 32-bit systems, there might be a use-after-free in the <code>kvm_debugregs</code> structure that could be copied to userspace, causing an information leak.
CVE-2023-1579	Heap based buffer overflow in <code>binutils-gdb/bfd/libbfd.c</code> in <code>bfd_getl64</code> .
CVE-2023-1611	A use-after-free flaw was found in <code>btrfs_search_slot</code> in <code>fs/btrfs/ctree.c</code> in <code>btrfs</code> in the Linux Kernel. This flaw allows a local attacker to cause a kernel information leak.
CVE-2023-1670	A flaw use after free in the Linux kernel Xircom 16-bit PCMCIA (PC-card) Ethernet driver was found. A local user can potentially escalate their privileges on the system.
CVE-2023-1829	A use-after-free vulnerability in the Linux Kernel traffic control index filter (tcindex) can be exploited to achieve local privilege escalation. The vulnerability exists in the <code>tcindex_delete</code> function which does not properly deactivate filters in case of a perfect hashes while deleting the underlaying structure. A local attacker user can use this vulnerability to elevate its privileges to root. We found a PoC exploit for this issue. CVE ID: 8c710f75256bb3cf05ac7b1672c82b92c43f3d28.
CVE-2023-1855	A use-after-free flaw was found in <code>xgene_hwmon_remove</code> in <code>drivers/hwmon/xgene-hwmon.c</code> in the Hardware Monitor. This flaw could allow a local attacker to crash the system due to a race problem. This vulnerability could even lead to a kernel information leak.
CVE-2023-1859	A use-after-free flaw was found in <code>xen_9pfs_front_remove</code> in <code>net/9p/trans_xen.c</code> in Xen transport for 9pfs in the Linux Kernel. This flaw could allow a local attacker to crash the system due to a race problem, possibly leading to a kernel information leak.
CVE-2023-1872	A use-after-free vulnerability in the Linux Kernel <code>io_uring</code> system can be exploited to achieve local privilege escalation. The presence of <code>ctx->uring_lock</code> which can lead to a Use-After-Free vulnerability due a race condition with fixed file table. This issue affects Linux Kernel: upgrading past commit da24142b1ef9fd5d36b76e36bab328a5b27523e8.
CVE-2023-1989	A use-after-free flaw was found in <code>btsdio_remove</code> in <code>drivers/bluetooth/btsdio.c</code> in the Linux Kernel. In this flaw, a local attacker can cause a race problem leading to a UAF on hdev devices.
CVE-2023-1990	A use-after-free flaw was found in <code>ndlc_remove</code> in <code>drivers/nfc/st-nci/ndlc.c</code> in the Linux Kernel. This flaw could allow a local attacker to cause a race problem.
CVE-2023-1998	The Linux kernel allows userspace processes to enable mitigations by calling <code>prctl</code> with <code>PR_SET_SPECULATION_CTRL</code> feature as well as by using <code>seccomp</code> . We had noticed that on VMs of at least one major cloud provider, the kernel speculation mitigations were disabled in some cases even after enabling the spectre-BTI mitigation with <code>prctl</code> . The same behavior can be observed on physical machines. The mitigation to IBRS on boot command line. This happened because when plain IBRS was enabled (not enhanced IBRS), the kernel determined that STIBP was not needed. The IBRS bit implicitly protects against cross-thread branch target injection. The STIBP bit was cleared on returning to userspace, due to performance reasons, which disabled the implicit STIBP and left the system vulnerable to branch target injection against which STIBP protects.
CVE-2023-20860	Spring Framework running version 6.0.0 - 6.0.6 or 5.3.0 - 5.3.25 using "*" as a pattern in Spring Security configuration can cause a mismatch in pattern matching between Spring Security and Spring MVC, and the potential for a security bypass.
CVE-2023-20861	In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, a local attacker can provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.
CVE-2023-21102	In <code>_efi_rt_asm_wrapper</code> of <code>efi-rt-wrapper.S</code> , there is a possible bypass of shadow stack protection due to a logic error. This issue affects Linux Kernel: escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. KernelAndroid ID: A-260821414References: Upstream kernel
CVE-2023-2162	A use-after-free vulnerability was found in <code>iscsi_sw_tcp_session_create</code> in <code>drivers/scsi/iscsi_tcp.c</code> in SCSI sub-component. A local attacker could leak kernel internal information.
CVE-2023-2163	Incorrect verifier pruning in BPF in Linux Kernel leads to unsafe code paths being incorrectly marked as safe. This issue affects Linux Kernel: 5.4 leads to unsafe code paths being incorrectly marked as safe, kernel memory, lateral privilege escalation, and container escape.
CVE-2023-2194	An out-of-bounds write vulnerability was found in the Linux kernel's SLIMpro I2C device driver. The userspace "count" variable was set to a number between 0-255 and was used as the size of a memcpy, possibly writing beyond the end of <code>dma_buffer</code> . This issue affects Linux Kernel: crash the system or potentially achieve code execution.

CVE-2023-22025	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, product of Oracle Java SE versions that are affected are Oracle Java SE: 8u381-perf, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11 and 21.3.7. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to access sensitive data in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:None/C:N/I:N/A:L).
CVE-2023-22067	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: C) are Oracle Java SE: 8u381, 8u381-perf; Oracle GraalVM Enterprise Edition: 20.3.11 and 21.3.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via CORBA to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start application or a web service. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:None/C:N/I:N/A:L).
CVE-2023-22081	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to access sensitive data in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:None/C:N/I:N/A:L).
CVE-2023-2283	A vulnerability was found in libssh, where the authentication check of the connecting client can be bypassed in the case of memory allocation problems. This issue may happen if there is insufficient memory or the memory usage is limited. The variable `rc` which is initialized to SSH_ERROR and later rewritten to save the return value of the function call `pki_key_public_blob` is not changed between this point and the cryptographic verification. Therefore any error between them can be bypassed.
CVE-2023-22998	In the Linux kernel before 6.0.3, drivers/gpu/drm/virtio/virtgpu_object.c misinterprets the drm_gem_shmem_get_size() in the error case, whereas it is actually an error pointer).
CVE-2023-23003	In the Linux kernel before 5.16, tools/perf/util/expr.c lacks a check for the hashmap__new return value.
CVE-2023-23039	An issue was discovered in the Linux kernel through 6.2.0-rc2. drivers/tty/vcc.c has a race condition and resultant use-after-free. An attacker removes a VCC device while calling open(), aka a race condition between vcc_open() and vcc_remove().
CVE-2023-23559	In rndis_query_oid in drivers/net/wireless/rndis_wlan.c in the Linux kernel through 6.1.5, there is an integer overflow.
CVE-2023-2454	schema_element defeats protective search_path changes; It was found that certain database calls in PostgreSQL could bypass database-level privileges to execute arbitrary code.
CVE-2023-2455	Row security policies disregard user ID changes after inlining; PostgreSQL could permit incorrect policies to be applied when a common user and query is planned initially and then re-used across multiple SET ROLES. Applying an incorrect policy could allow otherwise-forbidden reads and modifications. This affects only databases that have used CREATE POLICY to define row security policies.
CVE-2023-24998	Apache Commons FileUpload before 1.5 does not limit the number of request parts to be processed resulting in the application being vulnerable to a malicious upload or series of uploads. Note that, like all of the file upload limits, the new configuration option is enabled by default and must be explicitly configured.
CVE-2023-25012	The Linux kernel through 6.1.9 has a Use-After-Free in bigben_remove in drivers/hid/hid-bigbenff.c via a crafted USB device that remain registered for too long.
CVE-2023-25613	An LDAP Injection vulnerability exists in the <code>LDAPIdentityBackend</code> of Apache Kerby before 2.0.3. An attacker can inject LDAP queries into the <code>ldapUrl</code> parameter.
CVE-2023-2602	A vulnerability was found in the <code>pthread_create()</code> function in <code>libcap</code> . This issue may allow a malicious actor to use a process memory, which can exhaust the process memory.
CVE-2023-2603	A vulnerability was found in <code>libcap</code> . This issue occurs in the <code>_libcap_strdup()</code> function and can lead to an integer overflow.
CVE-2023-26159	Versions of the package follow-redirects before 1.15.4 are vulnerable to Improper Input Validation due to the <code>impr</code> function. When new URL() throws an error, it can be manipulated to misinterpret the hostname. An attacker could use this to redirect to a malicious site, potentially leading to information disclosure, phishing attacks, or other security breaches.
CVE-2023-26545	In the Linux kernel before 6.1.13, there is a double free in <code>net/mpls/af_mpls.c</code> upon an allocation failure (for registered devices) during the renaming of a device.
CVE-2023-27533	A vulnerability in input validation exists in <code>curl <8.0</code> during communication using the TELNET protocol may allow an attacker to bypass user name and "telnet options" during server negotiation. The lack of proper input scrubbing allows an attacker to send data without the application's intent. This vulnerability could be exploited if an application allows user input, thereby enabling an attacker to control the system.

CVE-2023-27535	An authentication bypass vulnerability exists in libcurl <8.0.0 in the FTP connection reuse feature that can result in subsequent transfers. Previously created connections are kept in a connection pool for reuse if they match the current configuration, such as CURLOPT_FTP_ACCOUNT, CURLOPT_FTP_ALTERNATIVE_TO_USER, CURLOPT_FTP_SSL_CCC, and CURLOPT_FTP_SSL_OPTIONS. These are included in the configuration match checks, causing them to match too easily. This could lead to libcurl using the wrong connection, potentially allowing unauthorized access to sensitive information.
CVE-2023-27536	An authentication bypass vulnerability exists libcurl <8.0.0 in the connection reuse feature which can reuse previous connections with incorrect user permissions due to a failure to check for changes in the CURLOPT_GSSAPI_DELEGATION option. This can allow negotiate/GSSAPI transfers and could potentially result in unauthorized access to sensitive information. The safest fix is to change the CURLOPT_GSSAPI_DELEGATION option has been changed.
CVE-2023-27538	An authentication bypass vulnerability exists in libcurl prior to v8.0.0 where it reuses a previously established SSH connection. An option was modified, which should have prevented reuse. libcurl maintains a pool of previously used connections to reuse if the configurations match. However, two SSH settings were omitted from the configuration check, allowing them to match and reuse an inappropriate connection.
CVE-2023-28321	An improper certificate validation vulnerability exists in curl <v8.1.0 in the way it supports matching of wildcard patterns in "Name" in TLS server certificates. curl can be built to use its own name matching function for TLS rather than one provided by the operating system. The wildcard matching function would match IDN (International Domain Name) hosts incorrectly and could as a result cause a mismatch. IDN hostnames are converted to puny code before used for certificate checks. Puny coded names always match the pattern match, but the wildcard check in curl could still check for `x*`, which would match even though the IDN host does not resemble an `x`.
CVE-2023-28322	An information disclosure vulnerability exists in curl <v8.1.0 when doing HTTP(S) transfers, libcurl might erroneously use the `CURLOPT_READFUNCTION` to ask for data to send, even when the `CURLOPT_POSTFIELDS` option has been used. This was used to issue a `PUT` request which used that callback. This flaw may surprise the application and cause it to not work or use memory after free or similar in the second transfer. The problem exists in the logic for a reused handle when it is used for a POST.
CVE-2023-28328	A NULL pointer dereference flaw was found in the az6027 driver in drivers/media/usb/dev-usb/az6027.c in the Linux kernel. The NULL pointer was not checked properly before transferring into the device. This flaw allows a local user to crash the system or potentially gain root access.
CVE-2023-28466	do_tls_getsockopt in net/tls/tls_main.c in the Linux kernel through 6.2.6 lacks a lock_sock call, leading to a race condition (NULL pointer dereference).
CVE-2023-28484	In libxml2 before 2.10.4, parsing of certain invalid XSD schemas can lead to a NULL pointer dereference and subsequent crash. The affected code is xmlSchemaFixupComplexType in xmlschemas.c.
CVE-2023-29469	An issue was discovered in libxml2 before 2.10.4. When hashing empty dict strings in a crafted XML document, xmlHash returns non-deterministic values, leading to various logic and memory errors, such as a double free. This behavior occurs because of an empty string, and any value is possible (not solely the `0` value).
CVE-2023-2985	A use after free flaw was found in hfsplus_put_super in fs/hfsplus/super.c in the Linux Kernel. This flaw could allow a local user to crash the system or potentially gain root access.
CVE-2023-30456	An issue was discovered in arch/x86/kvm/vmx/nested.c in the Linux kernel before 6.2.8. nVMX on x86_64 lacks a check for the VMXON bit in the VMXCR0 register.
CVE-2023-30772	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/power/supply/da9150-charger.c when unplugs a device.
CVE-2023-31081	An issue was discovered in drivers/media/test-drivers/vidtv/vidtv_bridge.c in the Linux kernel 6.2. There is a NULL pointer dereference in vidtv_mux_stop_thread. In vidtv_stop_streaming, after dvb->mux=NULL occurs, it executes vidtv_mux_stop_thread which dereferences dvb->mux.
CVE-2023-31083	An issue was discovered in drivers/bluetooth/hci_ldisc.c in the Linux kernel 6.2. In hci_uart_tty_ioctl, there is a race condition and HCIUARTGETPROTO. HCI_UART_PROTO_SET is set before hci->proto is set. A NULL pointer dereference occurs when hci->proto is NULL.
CVE-2023-3141	A use-after-free flaw was found in r592_remove in drivers/memstick/host/r592.c in media access in the Linux Kernel. This flaw could allow a local user to crash the system at device disconnect, possibly leading to a kernel information leak.
CVE-2023-3161	A flaw was found in the Framebuffer Console (fbcon) in the Linux Kernel. When providing font->width and font->height, since there are no checks in place, a shift-out-of-bounds occurs leading to undefined behavior and possible denial of service.
CVE-2023-3220	An issue was discovered in the Linux kernel through 6.1-rc8. dpu_crtc_atomic_check in drivers/gpu/drm/msm/disp/dpu1/dpu_crtc.c will cause the NULL Pointer Dereference.
CVE-2023-32269	An issue was discovered in the Linux kernel before 6.1.11. In net/netrom/af_netrom.c, there is a use-after-free because of a connected AF_NETROM socket. However, in order for an attacker to exploit this, the system must have netrom routing enabled and CAP_NET_ADMIN capability.
CVE-2023-33203	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/net/ethernet/qualcomm/emac/emac.c when unplugs an emac based device.
CVE-2023-33460	There's a memory leak in yajl 2.1.0 with use of yajl_tree_parse function. which will cause out-of-memory in server applications.

CVE-2023-33953	gRPC contains a vulnerability that allows hpack table accounting errors could lead to unwanted disconnects between →Three vectors were found that allow the following DOS attacks: - Unbounded memory buffering in the HPACK the HPACK parser The unbounded CPU consumption is down to a copy that occurred per-input-block in the parser to the memory copy bug we end up with an O(n^2) parsing loop, with n selected by the client. The unbounded mem check was behind the string reading code, so we needed to first buffer up to a 4 gigabyte string before rejecting it a have an encoding quirk whereby an infinite number of 0,Äs can be added at the start of an integer. gRPC,Äs hpa concluding a parse. - gRPC,Äs metadata overflow check was performed per frame, so that the following sequence HEADERS: containing a: 1 CONTINUATION: containing a: 2 CONTINUATION: containing a: 3 etc,Ä¶
CVE-2023-3397	A race condition occurred between the functions lmLogClose and txEnd in JFS, in the Linux Kernel, executed in d attacker with normal user privileges to crash the system or leak internal kernel information.
CVE-2023-34256	An issue was discovered in the Linux kernel before 6.3.3. There is an out-of-bounds read in crc16 in lib/crc16.c wh ext4_group_desc_csum does not properly check an offset. NOTE: this is disputed by third parties because the kern with the stated "When modifying the block device while it is mounted by the filesystem" access.
CVE-2023-3567	A use-after-free flaw was found in vcs_read in drivers/tty/vt/vc_screen.c in vc_screen in the Linux Kernel. This iss access to cause a system crash or leak internal kernel information.
CVE-2023-35823	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in saa7134_finidev in drivers
CVE-2023-35824	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in dm1105_remove in drivers
CVE-2023-35828	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in renesas_usb3_remove in d
CVE-2023-35829	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in rkvddec_remove in drivers/
CVE-2023-37453	An issue was discovered in the USB subsystem in the Linux kernel through 6.4.2. There is an out-of-bounds and cr sysfs.c.
CVE-2023-3772	A flaw was found in the Linux kernel,Äs IP framework for transforming packets (XFRM subsystem). This issue r CAP_NET_ADMIN privileges to directly dereference a NULL pointer in xfrm_update_ae_params(), leading to a p
CVE-2023-3773	A flaw was found in the Linux kernel,Äs IP framework for transforming packets (XFRM subsystem). This issue r CAP_NET_ADMIN privileges to cause a 4 byte out-of-bounds read of XFRMA_MTIMER_THRESH when parsin leakage of sensitive heap data to userspace.
CVE-2023-3777	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local nf_tables_delrule() is flushing table rules, it is not checked whether the chain is bound and the chain's owner rule c circumstances. We recommend upgrading past commit 6eaf41e87a223ae6f8e7a28d6e78384ad7e407f8.
CVE-2023-37788	goproxy v1.1 was discovered to contain an issue which can lead to a Denial of service (DoS) via unspecified vector
CVE-2023-38546	This flaw allows an attacker to insert cookies at will into a running program using libcurl, if the specific series of c In its API, an application creates 'easy handles' that are the individual handles for single transfers. libcurl provides called curl_easy_duphandle. If a transfer has cookies enabled when the handle is duplicated, the cookie-enable stat actual cookies. If the source handle did not read any cookies from a specific file on disk, the cloned version of the h as none (using the four ASCII letters, no quotes).Subsequent use of the cloned handle that does not explicitly set a inadvertently load cookies from a file named none - if such a file exists and is readable in the current directory of th correct file format of course.
CVE-2023-39189	A flaw was found in the Netfilter subsystem in the Linux kernel. The nfnl_osf_add_callback function did not valid This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, leading to a cra
CVE-2023-39192	A flaw was found in the Netfilter subsystem in the Linux kernel. The xt_u32 module did not validate the fields in t local privileged attacker to trigger an out-of-bounds read by setting the size fields with a value beyond the array bo disclosure.
CVE-2023-39193	A flaw was found in the Netfilter subsystem in the Linux kernel. The sctp_mt_check did not validate the flag_coun (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, leading to a crash or information disclosure.
CVE-2023-39194	A flaw was found in the XFRM subsystem in the Linux kernel. The specific flaw exists within the processing of sta the end of an allocated buffer. This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-o information disclosure.
CVE-2023-39197	An out-of-bounds read vulnerability was found in Netfilter Connection Tracking (conntrack) in the Linux kernel. T sensitive information via the DCCP protocol.
CVE-2023-39417	IN THE EXTENSION SCRIPT, a SQL Injection vulnerability was found in PostgreSQL if it uses @extowner@, @ quoting construct (dollar quoting, ", or ""). If an administrator has installed files of a vulnerable, trusted, non-bundl CREATE privilege can execute arbitrary code as the bootstrap superuser.
CVE-2023-40577	Alertmanager handles alerts sent by client applications such as the Prometheus server. An attacker with the permis alerts endpoint could be able to execute arbitrary JavaScript code on the users of Prometheus Alertmanager. This is 0.2.51.

CVE-2023-4206	A use-after-free vulnerability in the Linux kernel's net/sched: cls_route component can be exploited to achieve local privilege escalation. When tcf_unbind_filter() is called on an existing filter, the whole tcf_result struct is always copied into the new instance of the filter. This causes the filter to be added to a class, as tcf_unbind_filter() is always called on the old instance in the success path, decreasing filter_cnt of the filter. When the filter is deleted, leading to a use-after-free. We recommend upgrading past commit b80b829e9e2c1b3f7aae34855e04d8f6e.
CVE-2023-4207	A use-after-free vulnerability in the Linux kernel's net/sched: cls_fw component can be exploited to achieve local privilege escalation. When tcf_unbind_filter() is called on an existing filter, the whole tcf_result struct is always copied into the new instance of the filter. This causes the filter to be added to a class, as tcf_unbind_filter() is always called on the old instance in the success path, decreasing filter_cnt of the filter. When the filter is deleted, leading to a use-after-free. We recommend upgrading past commit 76e42ae831991c828cfa8c37736ebfb8.
CVE-2023-4208	A use-after-free vulnerability in the Linux kernel's net/sched: cls_u32 component can be exploited to achieve local privilege escalation. When tcf_unbind_filter() is called on an existing filter, the whole tcf_result struct is always copied into the new instance of the filter. This causes the filter to be added to a class, as tcf_unbind_filter() is always called on the old instance in the success path, decreasing filter_cnt of the filter. When the filter is deleted, leading to a use-after-free. We recommend upgrading past commit 3044b16e7c6fe5d24b1cdbc1bd0a9d92.
CVE-2023-42753	An array indexing vulnerability was found in the netfilter subsystem of the Linux kernel. A missing macro could lead to an out-of-bounds offset, providing attackers with the primitive to arbitrarily increment/decrement a memory buffer out-of-bound. This could be used to crash the system or potentially escalate their privileges on the system.
CVE-2023-42754	A NULL pointer dereference flaw was found in the Linux kernel ipv4 stack. The socket buffer (skb) was assumed to have __ip_options_compile, which is not always the case if the skb is re-routed by ipvs. This issue may allow a local user to crash the system.
CVE-2023-42755	A flaw was found in the IPv4 Resource Reservation Protocol (RSVP) classifier in the Linux kernel. The xprt pointer was not checked for NULL, leading to an out-of-bounds read in the `rsvp_classify` function. This issue may allow a local user to crash the system.
CVE-2023-42756	A flaw was found in the Netfilter subsystem of the Linux kernel. A race condition between IPSET_CMD_ADD and IPSET_CMD_DESTROY could lead to a panic due to the invocation of `__ip_set_put` on a wrong `set`. This issue may allow a local user to crash the system.
CVE-2023-43785	A vulnerability was found in libX11 due to a boundary condition within the _XkbReadKeySyms() function. This flaw allows an attacker to read out-of-bounds read error and read the contents of memory on the system.
CVE-2023-43786	A vulnerability was found in libX11 due to an infinite loop within the PutSubImage() function. This flaw allows an attacker to consume resources and cause a denial of service condition.
CVE-2023-43787	A vulnerability was found in libX11 due to an integer overflow within the XCreateImage() function. This flaw allows an attacker to execute arbitrary code with elevated privileges.
CVE-2023-44981	Authorization Bypass Through User-Controlled Key vulnerability in Apache ZooKeeper. If SASL Quorum Peer authentication is enabled (quorum.auth.enableSasl=true), the authorization is done by verifying that the instance part in SASL authentication matches the instance part in SASL auth ID. The instance part in SASL auth ID is optional and if it's missing, like 'eve@EXAMPLE.COM', the authorization check is bypassed. An arbitrary endpoint could join the cluster and begin propagating counterfeit changes to the leader, essentially giving the attacker control over the cluster. Quorum Peer authentication is not enabled by default. Users are recommended to upgrade to version 3.9.1, 3.9.2, or 4.0.0 to ensure the ensemble election/quorum communication is protected by a firewall as this will mitigate the issue. See the documentation for cluster administration.
CVE-2023-4569	A memory leak flaw was found in nft_set_catchall_flush in net/netfilter/nf_tables_api.c in the Linux Kernel. This is due to the double-deactivations of catchall elements, which can result in a memory leak.
CVE-2023-45862	An issue was discovered in drivers/usb/storage/ene_ub6250.c for the ENE UB6250 reader driver in the Linux kernel. The driver can extend beyond the end of an allocation.
CVE-2023-45871	An issue was discovered in drivers/net/ethernet/intel/igb/igb_main.c in the IGB driver in the Linux kernel before 6.0. The driver can process frames larger than the MTU.
CVE-2023-46120	The RabbitMQ Java client library allows Java and JVM-based applications to connect to and interact with RabbitMQ. When receiving Message objects, attackers could send a very large Message causing a memory overflow and triggering a denial of service. Users may suffer from DoS attacks from RabbitMQ Java client which will ultimately exhaust the memory of the consumer. Upgrade to version 5.18.0.
CVE-2023-46218	This flaw allows a malicious HTTP server to set "super cookies" in curl that are then passed back to more origins than intended. This allows a site to set cookies that then would get sent to different and unrelated sites and domains. It could do this by using the curl_setopt function that verifies a given cookie domain against the Public Suffix List (PSL). For example a cookie could be set for the domain 'lower case hostname `curl.co.uk`, even though `co.uk` is listed as a PSL domain.
CVE-2023-4622	A use-after-free vulnerability in the Linux kernel's af_unix component can be exploited to achieve local privilege escalation. When the function tries to add data to the last skb in the peer's rcv queue without locking the queue. Thus there is a race where the peer could access an skb locklessly that is being released by garbage collection, resulting in use-after-free. We recommend upgrading past commit 790c2f9d15b594350ae9bca7b236f2b1859de02c.
CVE-2023-4623	A use-after-free vulnerability in the Linux kernel's net/sched: sch_hfsc (HFSC qdisc traffic control) component can be exploited to achieve local privilege escalation. If a class with a link-sharing curve (i.e. with the HFSC_FSC flag set) has a parent without a link-sharing curve, the function on the parent, but vtree_remove() will be skipped in update_vf(). This leaves a dangling pointer that can cause a use-after-free. We recommend upgrading past commit b3d26c5702c7d6c45456326e56d2ccf3f103e60f.

CVE-2023-46343	In the Linux kernel before 6.5.9, there is a NULL pointer dereference in send_acknowledge in net/nfc/nci/spi.c.
CVE-2023-4921	A use-after-free vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. The attacker uses a class of the qfq qdisc, sending network packets triggers use-after-free in qfq_dequeue() due to the incorrect checking in agg_dequeue(). We recommend upgrading past commit 8fc134fee27f2263988ae38920bc03da416b03d.
CVE-2023-49295	quic-go is an implementation of the QUIC protocol (RFC 9000, RFC 9001, RFC 9002) in Go. An attacker can cause a denial of service by sending a large number of PATH_CHALLENGE frames. The receiver is supposed to respond to each PATH_CHALLENGE frame. The attacker can prevent the receiver from sending out (the vast majority of) these PATH_RESPONSE frames by causing the receiver to selectively acknowledging received packets) and by manipulating the peer's RTT estimate. This vulnerability has been resolved in version 0.39.4.
CVE-2023-49568	A denial of service (DoS) vulnerability was discovered in go-git versions prior to v5.11. This vulnerability allows an attacker to perform denial of service attacks by providing specially crafted responses from a Git server which triggers resource exhaustion in go-git→cli→transport→http→filesystem supported by go-git→cli→transport→http→filesystem are not affected by this vulnerability. This is a go-git→cli→transport→http→filesystem implementation issue and does not affect the upstream git→cli.
CVE-2023-49569	A path traversal vulnerability was discovered in go-git versions prior to v5.11. This vulnerability allows an attacker to traverse the filesystem. In the worse case scenario, remote code execution could be achieved. Applications are only affected if they use pkg.go.dev/github.com/go-git/go-billy/v5/osfs#ChrootOS , which is the default when using "Plain" versions of OpenSSH. Applications using BoundOS https://pkg.go.dev/github.com/go-git/go-billy/v5/osfs#BoundOS → or in-memory file systems are not affected. This is a go-git→cli→transport→http→filesystem implementation issue and does not affect the upstream git→cli.
CVE-2023-5043	Ingress nginx annotation injection causes arbitrary command execution.
CVE-2023-5044	Code injection via nginx.ingress.kubernetes.io/permanent-redirect annotation.
CVE-2023-51042	In the Linux kernel before 6.4.12, amdgpu_cs_wait_all_fences in drivers/gpu/drm/amd/amdgpu/amdgpu_cs.c has a use-after-free during a race condition between fence release and fence wait.
CVE-2023-51043	In the Linux kernel before 6.4.5, drivers/gpu/drm/drm_atomic.c has a use-after-free during a race condition between atomic commit and atomic unload.
CVE-2023-52438	In the Linux kernel, the following vulnerability has been resolved: binder: fix use-after-free in shrinker's callback The shrinker's callback, which means that using alloc->vma pointer isn't safe as it can race with munmap(). As of commit 8c1e1e1e ("binder: zap pages with read mmap_sem in munmap") the mmap lock is downgraded after the vma has been isolated. I was manually adding some delays and triggering page reclaiming through the shrinker's debug sysfs. The following KASAN report shows the bug: BUG: KASAN: slab-out-of-bounds in __do_softirq+0x470/0x4b8 Read of size 8 at addr ffff356ed50e50f0 by task bash/478 CPU: 1 PID: 478 Comm: bash Not tainted 6.4.0-rc1-gcc #70 Hardware name: linux,dummy-virt (DT) Call trace: zap_page_range_single+0x470/0x4b8 binder_alloc_free_page+0x130/0x3b0 list_lru_walk_node+0xc4/0x22c binder_shrink_scan+0x108/0x1dc shrinker_debugfs_scan_write+0x10/0x1c vfs_write+0x1ac/0x758 ksys_write+0xf0/0x1dc __arm64_sys_write+0x6c/0x9c Allocated by task 492: kmem_cache_alloc+0x2c/0x190 mmap_region+0x258/0x18bc do_mmap+0x694/0xa60 vm_mmap_pgoff+0x170/0x29c ksys_mmap+0x10/0x2c __do_softirq+0xcc/0x144 Freed by task 491: kmem_cache_free+0x17c/0x3c8 vm_area_free_rcu_cb+0x74/0x98 rcu_core+0xa3/0x100 __do_softirq+0x2fc/0xd24 Last potentially related work creation: __call_rcu_common.constprop.0+0x6c/0xba0 call_rcu+0x10/0x2c remove_vma+0xe4/0x118 do_vmi_align_munmap.isra.0+0x718/0xb5c do_vmi_munmap+0xdc/0x1fc __vm_munmap+0x58/0x7c Fix this issue by performing instead a vma_lookup() which will fail to find the vma that was isolated by the shrinker. That this option has better performance than upgrading to a mmap write lock which would increase contention. Plus, the old option was removed anyway.
CVE-2023-52439	In the Linux kernel, the following vulnerability has been resolved: uio: Fix use-after-free in uio_open core-1 core-2 ----- uio_unregister_device uio_open idev = idr_find() device_unregister(&idev) kfree(idev) >dev) uio_device_release get_device(&idev->dev) kfree(idev) uio_free_minor(minor) uio_release put_device(&idev) ----- In the core-1 uio_unregister_device(), the device_unregister will kfree the idev. But after core-1 device_unregister, put_device and before doing kfree, the core-2 may get_device. Then: 1. After core-2 get_device, kfree for idev. 2. When core-2 do uio_release and put_device, the idev will be double freed. To address this issue, we need to hold the idev with minor_lock.
CVE-2023-52456	In the Linux kernel, the following vulnerability has been resolved: serial: imx: fix tx statemachine deadlock When the TX_EN pin of the tx statemachine is used to control the RTS pin to drive the RS485 transceiver TX_EN pin. When the TTY port is closed (for instance during userland application crash), imx_uart_shutdown disables the interface and disables the Transmitter. When imx_uart_stop_tx bails on an incomplete transmission, to be retrigged by the TC interrupt. This interrupt is disabled when the TX_EN transitions out of SEND. The statemachine is in deadlock now, and the TX_EN remains low, making the interface unusable. This patch fixes incomplete transmission AND whether TC interrupts are enabled before bailing to be retrigged. This makes sure the TX_EN is properly set to WAIT_AFTER_SEND.
CVE-2023-52462	In the Linux kernel, the following vulnerability has been resolved: bpf: fix check for attempt to corrupt spilled pointer In the bpf verifier, a 1/2/4-byte register, we set slot_type[BPF_REG_SIZE - 1] (plus potentially few more below it, depending on actual register size). If we have spilled register we need to consult slot_type[7], not slot_type[0]. To avoid the need to remember and double-check the register type, we help.
CVE-2023-52467	In the Linux kernel, the following vulnerability has been resolved: mfd: syscon: Fix null pointer dereference in of_syscon_get_res to dynamically allocated memory which can be NULL upon failure.

CVE-2023-52477	In the Linux kernel, the following vulnerability has been resolved: usb: hub: Guard against accesses to uninitialized usb/core/hub.c and drivers/usb/core/hub.h access fields inside udev->bos without checking if it was allocated and if for whatever reason, udev->bos will be NULL and those accesses will result in a crash: BUG: kernel NULL pointer dereference at 0000000000000000 [1] PREEMPT SMP NOPTI CPU: 5 PID: 17818 Comm: kworker/5:1 Tainted: G W 5.15.0-rc7-glibc (4.19.0-rc7) Hardware name: Google Kindred/Kindred, BIOS Google_Kindred.12672.413.0 02/03/2021 Workaround: 0010:hub_port_reset+0x193/0x788 Code: 89 f7 e8 20 f7 15 00 48 8b 43 08 80 b8 96 03 00 00 03 75 36 0f b7 88 92 a8 03 00 00 <48> 83 78 18 00 74 19 48 89 df 48 8b 75 b0 ba 02 00 00 00 4c 89 e9 RSP: 0018:ffffab740c53fc8 EFEB RBX: ffffffa1bc5f678000 RCX: 00000000000000310 RDX: ffffffffdfdf RSI: 0000000000000286 RDI: ffffffa1be96000001b7d5edaa20c R09: ffffffff005e060 R10: 0000000000000001 R11: 0000000000000000 R12: 0000000000000000 R13: 0000000000000032 R15: 0000000000000000 FS: 0000000000000000(0000) GS: fffffa1be96540000(0000) knlGS: 0000000000000000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000018 CR3: 0000000022e80c005 CR4: 00000000003706e0 hub_activate+0x5b7/0x68f process_one_work+0x1a2/0x487 worker_thread+0x11a/0x288 kthread+0x13a/0x152 ? kthread_associate_blkcg+0x70/0x70 ret_from_fork+0x1f/0x30 Fall back to a default behavior if the BOS descriptor functionalities that depend on it: LPM support checks, Super Speed capability checks, U1/U2 states setup.
CVE-2023-52480	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix race condition between session lookup and session setup ksmbd_session_lookup smb2_sess_setup sess = xa_load xa_erase(&conn->sessions, sess->id); ksmbd_session_lookup sess->last_active = jiffies + This patch add rwsem to fix race condition between ksmbd_session_lookup and ksmbd_session_setup
CVE-2023-52484	In the Linux kernel, the following vulnerability has been resolved: iommu/arm-smmu-v3: Fix soft lockup triggered by arm_smmu_cmdq_issue_cmdlist When running an SVA case, the following soft lockup is triggered: ----- CPU#244 stuck for 26s! pstate: 83400009 (Nzcv daif +PAN -UAO +TCO +DIT -SSBS BTYPE=) pc : arm_smmu_cmdq_issue_cmdlist lr : arm_smmu_cmdq_issue_cmdlist+0x150/0xa50 sp : fffff8000d83ef290 x29: fffff8000d83ef290 x28: 000000003b26 fffff8000d83ef3c0 x25: da86c0812194a0e8 x24: 0000000000000000 x23: 0000000000000040 x22: fffff8000d83ef3c0 x20: 0000000000000001 x19: fffff000c6398080 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000000000000 x14: fffff3000b4a30888 x13: fffff3000b4a3cf60 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x7: 0000000000000000 x6: 00000000000048cfa x5: 0000000000000000 x4: 0000000000000000 x1: 0000000000000000 x0: 0000000000000001 Call trace: arm_smmu_cmdq_issue_cmdlist+0x118/0x254 arm_smmu_tlb_inv_range_asid+0x6c/0x130 arm_smmu_mm_invalidate_range+0xa0/0xa4 __mmu_invalidate_range+0x88/0x120 unmap_vmas+0x194/0x1e0 unmap_region+0xb4/0x144 do_mas_align_munmap+0x290/0x490 do_munmap+0xa8/0x19c __arm64_sys_munmap+0x28/0x50 invoke_syscall+0x78/0x11c el0_svc_common.constprop.0+0x58 el0_svc_common+0x2c/0xd4 el0t_64_sync_handler+0x114/0x140 el0t_64_sync+0x1a4/0x1a8 ----- rc1 the arm_smmu_mm_invalidate_range above is renamed to "arm_smmu_mm_arch_invalidate_secondary_tlbs", 06ff87bae8d3 ("arm64: mm: remove unused functions and variable prototypes") fixed a similar lockup on the CPU too, since arm_smmu_mm_arch_invalidate_secondary_tlbs() is called typically next to MMU tlb flush function, e.g. { __flush_tlb_range { // check MAX_TLBI_OPS } } mmu_notifier_arch_invalidate_secondary_tlbs { arm_smmu_invalidate_range { // check MAX_TLBI_OPS } } } Clone a CMDQ_MAX_TLBI_OPS from the MAX_TLBI_OPS in tlbflush.h, since it's a page table, so it makes sense to align with the tlbflush code. Then, replace per-page TLBI commands with a single hit this threshold.
CVE-2023-52494	In the Linux kernel, the following vulnerability has been resolved: bus: mhi: host: Add alignment check for event ring read pointer by "is_valid_ring_ptr" to make sure it is in the buffer range, but there is another risk the pointer expecting event ring elements are 128 bits(struct mhi_ring_element) aligned, an unaligned read pointer could lead to memory corruption. So add a alignment check for event ring read pointer.
CVE-2023-52502	In the Linux kernel, the following vulnerability has been resolved: net: nfc: fix races in nfc_llcp_sock_get() and nfc_llcp_sock_put() race in nfc_llcp_sock_get(), leading to UAF. Getting a reference on the socket found in a lookup while holding a lock nfc_llcp_sock_get_sn() has a similar problem. Finally nfc_llcp_rcv_sn() needs to make sure the socket found by nfc_llcp_sock_get_sn() is not NULL.
CVE-2023-52503	In the Linux kernel, the following vulnerability has been resolved: tee: amdtee: fix use-after-free vulnerability in amdtee_close_session condition in amdtee_close_session that may cause use-after-free in amdtee_open_session. For instance, if a session is closed via kref_put(&sess->refcount, destroy_session); the reference count will get decremented, and the session is freed. However, if in another thread, amdtee_open_session() is called before destroy_session() has completed execution, the session is freed up later in destroy_session() leading to use-after-free in amdtee_open_session. To fix this issue, treat decrementing the reference count from session list in destroy_session() as a critical section, so that it is executed atomically.
CVE-2023-52507	In the Linux kernel, the following vulnerability has been resolved: nfc: nci: assert requested protocol is valid The protocol is supported. Assert the provided protocol is less than the maximum defined so it doesn't potentially produce a clearer error for undefined protocols vs unsupported ones.
CVE-2023-52509	In the Linux kernel, the following vulnerability has been resolved: ravb: Fix use-after-free issue in ravb_tx_timeout call cancel_work_sync(). Otherwise, ravb_tx_timeout_work() is possible to use the freed priv after ravb_remove() is called. ravb_tx_timeout() ravb_remove() unregister_netdev() free_netdev(ndev) // free priv ravb_tx_timeout_work() // use priv so that ravb_stop() is called. And, after phy_stop() is called, netif_carrier_off() is also called. So that .ndo_tx_timeout is called.
CVE-2023-52510	In the Linux kernel, the following vulnerability has been resolved: ieee802154: ca8210: Fix a potential UAF in ca8210_unregister_ext_clock(), it calls clk_unregister() to release priv->clk and returns an error. However, the caller expects an error where priv->clk is freed again in ca8210_unregister_ext_clock(). In this case, a use-after-free may happen in the session list by removing the first clk_unregister(). Also, priv->clk could be an error code on failure of clk_register_fixed_rate() in ca8210_unregister_ext_clock().

CVE-2023-52513	In the Linux kernel, the following vulnerability has been resolved: RDMA/siw: Fix connection failure handling In the newly created endpoint unlinks the listening endpoint and is ready to be dropped. This special case was not handling TCP socket close, causing a NULL dereference crash in siw_cm_work_handler() when dereferencing a NULL listener timeout, if immediate MPA request processing fails. This patch furthermore simplifies MPA processing in general: sk_data_ready() upcall is now suppressed, if the socket is already moved out of TCP_ESTABLISHED state.
CVE-2023-52524	In the Linux kernel, the following vulnerability has been resolved: net: nfc: llcp: Add lock when modifying device held when modifying it, or the list could become corrupted, as syzbot discovered.
CVE-2023-52525	In the Linux kernel, the following vulnerability has been resolved: wifi: mwifiex: Fix oob check condition in mwifiex_path trying to access the rfc1042 headers when the buffer is too small, so the driver can still process packets without
CVE-2023-52527	In the Linux kernel, the following vulnerability has been resolved: ipv4, ipv6: Fix handling of transhdrlen in __ip{, transhdrlen in length is a problem when the packet is partially filled (e.g. something like send(MSG_MORE) happens to an IPv4 or IPv6 packet as we don't want to repeat the transport header or account for it twice. This can happen upon splicing into an L2TP socket. The symptom observed is a warning in __ip6_append_data(): WARNING: CPU: 1 P1 __ip6_append_data.isra.0+0x1be8/0x47f0 net/ipv6/ip6_output.c:1800 that occurs when MSG_SPLICE_PAGES is partially occupied skbuff. The warning occurs when 'copy' is larger than the amount of data in the message iterator, includes the transport header length when it shouldn't. This can be triggered by, for example: sfd = socket(AF_INET, bind(sfd, ...); // ::1 connect(sfd, ...); // ::1 port 7 send(sfd, buffer, 4100, MSG_MORE); sendfile(sfd, dfd, NULL, 10 into the length if the write queue is empty in l2tp_ip6_sendmsg(), analogously to how UDP does things. l2tp_ip_sendmsg problem as it builds the UDP packet itself.
CVE-2023-52528	In the Linux kernel, the following vulnerability has been resolved: net: usb: smsc75xx: Fix uninit-value access in the following uninit-value access issue: ===== in smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] BUG: KMSAN: uninit-value in smsc75xx_bind+smmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/dump_stack+0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+0x1e/0x20 smsc75xx_wait_ready drivers/net/usb/msmc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/msmc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Google Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump

CVE-2023-52573	In the Linux kernel, the following vulnerability has been resolved: net: rds: Fix possible NULL-pointer dereference check, if conn pointer exists before dereferencing it as rdma_set_service_type() argument Found by Linux Verifica
CVE-2023-52574	In the Linux kernel, the following vulnerability has been resolved: team: fix null-ptr-deref when team device type is with reproducer [1]. BUG: kernel NULL pointer dereference, address: 000000000000228 ... RIP: 0010:vlan_dev... Trace: <TASK> ? __die+0x24/0x70 ? page_fault_oops+0x82/0x150 ? exc_page_fault+0x69/0x150 ? asm_exc_page_fault+0x35/0x140 [8021q] ? vlan_dev_hard_header+0x8e/0x140 [8021q] neigh_connected_output+0xb2/0x100 ip6_finish_output+0x43/0xc0 ? ip6_mtu+0x46/0x80 ip6_finish_output+0x2a/0xb0 mld_sendpack+0x18f/0x250 mld_ifc_work+0x35/0x40 worker_thread+0x4d/0x2f0 ? __pfx_worker_thread+0x10/0x10 kthread+0xe5/0x120 ? __pfx_kthread+0x10/0x10 ? __ret_from_fork_asm+0x1b/0x30 [1] \$ teamd -t team0 -d -c '{"runner": {"name": "loadbalance"}}' \$ ip link add link t-dummy name t-dummy.100 type vlan add name t-nlmon type nlmon \$ ip link set t-nlmon type nlmon \$ ip link set t-dummy up \$ ip link set team0 up \$ ip link set t-dummy.100 down \$ ip link set t-dummy.100 master t-dummy device and team device type is changed from non-ether to ether, header_ops of team device is changed to vlan_header_ops null-ptr-deref for vlan->real_dev in vlan_dev_hard_header() because team device is not a vlan device. Cache eth_header_ops cached header_ops to header_ops of team net device when its type is changed from non-ether to ether to fix the bug
CVE-2023-52577	In the Linux kernel, the following vulnerability has been resolved: dccp: fix dccp_v4_err()/dccp_v6_err() again dh... "struct dccp_hdr", not in the "byte 7" as Jann claimed. We need to make sure the ICMP messages are big enough, u... assumptions). syzbot reported: BUG: KMSAN: uninit-value in pskb_may_pull_reason include/linux/skbuff.h:2667 pskb_may_pull include/linux/skbuff.h:2681 [inline] BUG: KMSAN: uninit-value in dccp_v6_err+0x426/0x1aa0 net/core/include/linux/skbuff.h:2667 [inline] pskb_may_pull include/linux/skbuff.h:2681 [inline] dccp_v6_err+0x426/0x1aa0 net/core+0x4c7/0x880 net/ipv6/icmp.c:867 icmpv6_rcv+0x19d5/0x30d0 ip6_protocol_deliver_rcu+0xda6/0x2a60 net/ipv6/netfilter/ip6_input.c:483 [inline] NF_HOOK include/linux/netfilter.h:304 [inline] ip6_input+0x15d/0x430 net/ipv6/ip6_input.c:586 dst_input include/net/dst.h:468 [inline] ip6_rcv_finish+0x5db/0x870 net/ipv6/ip6_input.c:79 [inline] ipv6_rcv+0xda/0x390 net/ipv6/ip6_input.c:310 __netif_receive_skb_one_core net/core/dev.c:5523 [inline] netif_receive_skb_core/dev.c:5637 netif_receive_skb_internal net/core/dev.c:5723 [inline] netif_receive_skb+0x58/0x660 net/core/dev.c:5723 tun_get_user+0x564c/0x6940 drivers/net/tun.c:2002 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2048 call_vfs_write fs/read_write.c:491 [inline] vfs_write+0x8ef/0x15c0 fs/read_write.c:584 ksys_write+0x20f/0x4c0 fs/read_write.c:649 [inline] __se_sys_write fs/read_write.c:646 [inline] __x64_sys_write+0x93/0xd0 fs/read_write.c:common.c:50 [inline] do_syscall_64+0x41/0xc0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe_0 net/core/slab_post_alloc_hook+0x12f/0xb70 mm/slab.h:767 slab_alloc_node mm/slub.c:3478 [inline] kmem_cache_alloc_node kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:559 __alloc_skb+0x318/0x740 net/core/skbuff.c:650 alloc_skb_inet alloc_skb_with_frags+0xc8/0xbd0 net/core/skbuff.c:6313 sock_alloc_send_skb+0xa80/0xbf0 net/core/sock.c:279 [inline] tun_get_user+0x23cf/0x6940 drivers/net/tun.c:1846 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:204 [inline] new_sync_write fs/read_write.c:491 [inline] vfs_write+0x8ef/0x15c0 fs/read_write.c:584 ksys_write+0x20f/0x4c0 fs/read_write.c:649 [inline] __se_sys_write fs/read_write.c:646 [inline] __x64_sys_write+0x93/0xd0 fs/read_write.c:common.c:50 [inline] do_syscall_64+0x41/0xc0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe_0 syz-executor153 Not tainted 6.6.0-rc1-syzkaller-00014-ga747acc0b752 #0 Hardware name: Google Google Compute Engine Google 08/04/2023
CVE-2023-52578	In the Linux kernel, the following vulnerability has been resolved: net: bridge: use DEV_STATS_INC() syzbot/KC... br_handle_frame_finish() [1] This function can run from multiple cpus without mutual exclusion. Adopt SMP safe... >stats fields. Handles updates to dev->stats.tx_dropped while we are at it. [1] BUG: KCSAN: data-race in br_handle_frame_write to 0xffff8881374b2178 of 8 bytes by interrupt on cpu 1: br_handle_frame_finish+0xd4f/0xef0 net/bridge/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing_finish_ipv6+0x50f/0x540 NF_HOOK include/linux/netfilter.h:304 [inline] br_nf_pre_routing_finish_ipv6 net/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing+0x526/0xba0 net/bridge/br_netfilter_hooks.c:508 nf_hook_entry [inline] nf_hook_bridge_pre net/bridge/br_input.c:272 [inline] br_handle_frame+0x4c9/0x940 net/bridge/br_input.c:417 __netif_receive_skb_core net/core/dev.c:5417 __netif_receive_skb_one_core net/core/dev.c:5521 [inline] __netif_receive_skb_core process_backlog+0x21f/0x380 net/core/dev.c:5965 __napi_poll+0x60/0x3b0 net/core/dev.c:6527 napi_poll net/core/dev.c:6527 __do_softirq+0xc1/0x265 kernel/softirq.c:553 run_ksoftirqd+0x17/0x20 kernel/softirq.c:553 kthread+0x30a/0x4a0 kernel/smpboot.c:164 kthread+0x1d7/0x210 kernel/kthread.c:388 ret_from_fork+0x48/0x60 arch/x86/entry/entry_64.S:304 read-write to 0xffff8881374b2178 of 8 bytes by interrupt on cpu 0: br_handle_frame_finish+0xd4f/0xef0 net/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing_finish_ipv6+0x50f/0x540 NF_HOOK include/linux/netfilter.h:304 [inline] br_nf_pre_routing_finish_ipv6 net/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing+0x526/0xba0 net/bridge/br_netfilter_hooks.c:508 nf_hook_entry [inline] nf_hook_bridge_pre net/bridge/br_input.c:272 [inline] br_handle_frame+0x4c9/0x940 net/bridge/br_input.c:417 __netif_receive_skb_core net/core/dev.c:5417 __netif_receive_skb_one_core net/core/dev.c:5521 [inline] __netif_receive_skb_core process_backlog+0x21f/0x380 net/core/dev.c:5965 __napi_poll+0x60/0x3b0 net/core/dev.c:6527 napi_poll net/core/dev.c:6527 __do_softirq+0xc1/0x265 kernel/softirq.c:553 run_ksoftirqd+0x17/0x20 kernel/softirq.c:553 kthread+0x30a/0x4a0 kernel/smpboot.c:164 kthread+0x1d7/0x210 kernel/kthread.c:388 ret_from_fork+0x48/0x60 arch/x86/entry/entry_64.S:304 read-write to 0xffff8881374b2178 of 8 bytes by interrupt on cpu 0: br_handle_frame_finish+0xd4f/0xef0 net/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing_finish_ipv6+0x50f/0x540 NF_HOOK include/linux/netfilter.h:304 [inline] br_nf_pre_routing_finish_ipv6 net/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing+0x526/0xba0 net/bridge/br_netfilter_hooks.c:508 nf_hook_entry [inline] nf_hook_bridge_pre net/bridge/br_input.c:272 [inline] br_handle_frame+0x4c9/0x940 net/bridge/br_input.c:417 __netif_receive_skb_core net/core/dev.c:5417 __netif_receive_skb_one_core net/core/dev.c:5521 [inline] __netif_receive_skb_core process_backlog+0x21f/0x380 net/core/dev.c:5965 __napi_poll+0x60/0x3b0 net/core/dev.c:6527 napi_poll net/core/dev.c:6527 __do_softirq+0xc1/0x265 kernel/softirq.c:553 run_ksoftirqd+0x17/0x20 kernel/softirq.c:553 kthread+0x30a/0x4a0 kernel/smpboot.c:164 kthread+0x1d7/0x210 kernel/kthread.c:388 ret_from_fork+0x48/0x60 arch/x86/entry/entry_64.S:304 read-write to 0xffff8881374b2178 of 8 bytes by interrupt on cpu 0: br_handle_frame_finish+0xd4f/0xef0 net/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing_finish_ipv6+0x50f/0x540 NF_HOOK include/linux/netfilter.h:304 [inline] br_nf_pre_routing_finish_ipv6 net/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing+0x526/0xba0 net/bridge/br_netfilter_hooks.c:508 nf_hook_entry [inline] nf_hook_bridge_pre net/bridge/br_input.c:272 [inline] br_handle_frame+0x4c9/0x940 net/bridge/br_input.c:417 __netif_receive_skb_core net/core/dev.c:5417 __netif_receive_skb_one_core net/core/dev.c:5521 [inline] __netif_receive_skb_core process_backlog+0x21f/0x380 net/core/dev.c:5965 __napi_poll+0x60/0x3b0 net/core/dev.c:6527 napi_poll net/core/dev.c:6527 __do_softirq+0xc1/0x265 kernel/softirq.c:553 run_ksoftirqd+0x17/0x20 kernel/softirq.c:553 kthread+0x30a/0x4a0 kernel/smpboot.c:164 kthread+0x1d7/0x210 kernel/kthread.c:388 ret_from_fork+0x48/0x60 arch/x86/entry/entry_64.S:304 read-write to 0xffff8881374b2178 of 8 bytes by interrupt on cpu 0: br_handle_frame_finish+0xd4f/0xef0 net/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing_finish_ipv6+0x50f/0x540 NF_HOOK include/linux/netfilter.h:304 [inline] br_nf_pre_routing_finish_ipv6 net/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing+0x526/0xba0 net/bridge/br_netfilter_hooks.c:508 nf_hook_entry [inline] nf_hook_bridge_pre net/bridge/br_input.c:272 [inline] br_handle_frame+0x4c9/0x940 net/bridge/br_input.c:417 __netif_receive_skb_core net/core/dev.c:5417 __netif_receive_skb_one_core net/core/dev.c:5521 [inline] __netif_receive_skb_core process_backlog+0x21f/0x380 net/core/dev.c:5965 __napi_poll+0x60/0x3b0 net/core/dev.c:6527 napi_poll net/core/dev.c:6527 __do_softirq+0xc1/0x265 kernel/softirq.c:553 run_ksoftirqd+0x17/0x20 kernel/softirq.c:553 kthread+0x30a/0x4a0 kernel/smpboot.c:164 kthread+0x1d7/0x210 kernel/kthread.c:388 ret_from_fork+0x48/0x60 arch/x86/entry/entry_64.S:304 read-write to 0xffff8881374b2178 of 8 bytes by interrupt on cpu 0: br_handle_frame_finish+0xd4f/0xef0 net/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing_finish_ipv6+0x50f/0x540 NF_HOOK include/linux/netfilter.h:304 [inline] br_nf_pre_routing_finish_ipv6 net/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing+0x526/0xba0 net/bridge/br_netfilter_hooks.c:508 nf_hook_entry [inline] nf_hook_bridge_pre net/bridge/br_input.c:272 [inline] br_handle_frame+0x4c9/0x940 net/bridge/br_input.c:417 __netif_receive_skb_core net/core/dev.c:5417 __netif_receive_skb_one_core net/core/dev.c:5521 [inline] __netif_receive_skb_core process_backlog+0x21f/0x38

CVE-2023-52608	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Check mailbox/SMT channel completion interrupt the shared memory area is accessed to retrieve the message header at first and then, if the message which is still pending, the related payload is fetched too. When an SCMI command times out the channel ownership is given back to the agent and a late reply is received and, as a consequence, any further transmission attempt remains pending, waiting for the channel. Once that late reply is received the channel ownership is given back to the agent and any pending request is then allocated in the area of the just delivered late reply; then the wait for the reply to the new request starts. It has been observed that the channel can be wrongly associated with the freshly enqueued request: when that happens the SCMI stack in-flight lookup for the message header now present in the SMT area is related to the new pending transaction, even though the real reply belongs to the A2P channel can be detected by looking at the channel status bits: a genuine reply from the platform will have a completion IRQ. Add a consistency check to validate such condition in the A2P ISR.
CVE-2023-52628	In the Linux kernel, the following vulnerability has been resolved: netfilter: nftables: exthdr: fix 4-byte stack OOB. dst[len / 4] can write past the destination array which leads to stack corruption. This construct is necessary to clean up NOT a multiple of the register size, so make it conditional just like nft_payload.c does. The bug was added in 4.1 c and ip option support was added. Bug reported by Zero Day Initiative project (ZDI-CAN-21950, ZDI-CAN-21951).
CVE-2023-52654	In the Linux kernel, the following vulnerability has been resolved: io_uring/af_unix: disable sending io_uring over sockets. Lots of problems for io_uring in the past, and it still doesn't work exactly right and races with unix_stream_read_generic. disallow sending io_uring files via sockets via SCM_RIGHT, so there are no possible cycles involving registered files and the io_uring side unnecessary.
CVE-2023-52655	In the Linux kernel, the following vulnerability has been resolved: usb: aqc111: check packet for fixup for true limit. 0 and sizeof(u64) the value passed to skb_trim() as length will wrap around ending up as some very large value. The packet is located at that position, which will either oops or process some random value. The fix is to check against sizeof(u64) does. The issue exists since the introduction of the driver.
CVE-2023-52670	In the Linux kernel, the following vulnerability has been resolved: rpmsg: virtio: Free driver_override when rpmsg_remove() when rpmsg_remove(), otherwise the following memory leak will occur: unreferenced object 0xffff0000d55d7080 (size 16) pid 56, jiffies 4294893188 (age 214.272s) hex dump (first 32 bytes): 72 70 6d 73 67 5f 6e 73 00 backtrace: [<000000009c94c9c1>] __kmem_cache_alloc_node+0x1f3 [<0000000000000000>] kcalloc+0x10 [<0000000000000000>] kmalloc_node_track_caller+0x44/0x70 [<000000000228a60c3>] kstrndup+0x4c/0x90 [<0000000007158695>] driver_override_get+0x10 [<0000000003e9c4ea5>] rpmsg_register_device_override+0x98/0x170 [<0000000001c0c89a8>] rpmsg_ns_register_device+0x10 [<0000000000000000>] rpmsg_probe+0x2e0/0x3ec [<000000000e65a68df>] virtio_dev_probe+0x1c0/0x280 [<000000000443331cc>] really_probe+0x10 [<0000000000000000>] __driver_probe_device+0x78/0xe0 [<000000000a41c9a5b>] driver_probe_device+0xd8/0x160 [<0000000009c3bd5f>] __device_attach+0x10 [<00000000043cd7614>] bus_for_each_drv+0x7c/0xd4 [<0000000003b929a36>] __device_attach+0x9c/0x19c [<0000000000000000>] device_attach+0x14/0x20 [<0000000003c999637>] bus_probe_device+0xa0/0xac
CVE-2023-52672	In the Linux kernel, the following vulnerability has been resolved: pipe: wakeup wr_wait after setting max_usage. ("pipe: notification queue support") a regression was introduced that would lock up resized pipes under certain conditions. The fix for this is to move resizing the pipe ring size was moved to a different function, doing that moved the wakeup for pipe->wr_wait before the pipe was full before the resize occurred it would result in the wakeup never actually triggering pipe_write. Set @max_usage to 0 if writers if this isn't a watch queue. [Christian Brauner <brauner@kernel.org>: rewrite to account for watch queues]
CVE-2023-52675	In the Linux kernel, the following vulnerability has been resolved: powerpc/imc-pmu: Add a null pointer check in imc_pmu. Add a pointer to dynamically allocated memory which can be NULL upon failure.
CVE-2023-52677	In the Linux kernel, the following vulnerability has been resolved: riscv: Check if the code to patch lies in the exit region. vmalloc_to_page() which panics since the address does not lie in the vmalloc region.
CVE-2023-52682	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to wait on block writeback for post_read. If the file is not encrypted, it missed to call f2fs_wait_on_block_writeback() to wait for GCed page writeback in IPU write path. - do_garbage_collect - gc_data_segment - move_data_block - f2fs_submit_page_write migrate normal cluster's block. - f2fs_write_single_data_page - f2fs_do_write_data_page - f2fs_inplace_write_data - f2fs_submit_page_bio IRQ - f2fs_read_end_io data due to out-of-order GC and common IO. - f2fs_read_end_io
CVE-2023-52686	In the Linux kernel, the following vulnerability has been resolved: powerpc/powernv: Add a null pointer check in powernv. Add a pointer to dynamically allocated memory which can be NULL upon failure.
CVE-2023-52690	In the Linux kernel, the following vulnerability has been resolved: powerpc/powernv: Add a null pointer check to powernv. Add a pointer to dynamically allocated memory which can be NULL upon failure. Add a null pointer check, and release 'v'.
CVE-2023-52691	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: fix a double-free in si_dpm_init. When the driver is loaded, si_dpm_init is called. It calls si_dpm_dyn_state.vddc_dependency_on_dispclk.entries fails, amdgpu_free_extended_power_table is called to free the power table. When the control flow returns to si_dpm_sw_init, it goes to label dpm_failed and calls si_dpm_fini, which calls amdgpu_free_extended_power_table again. Thus a double-free is triggered.
CVE-2023-52693	In the Linux kernel, the following vulnerability has been resolved: ACPI: video: check for error while searching for parent. When called in acpi_video_dev_register_backlight() fails, for example, because acpi_ut_acquire_mutex() fails inside acpi_video_dev_register_backlight() (uninitialized) acpi_parent handle being passed to acpi_get_pci_dev() for detecting the parent pci device. Check acpi_status only in case of success. Found by Linux Verification Center (linuxtesting.org) with SVACE.

84

CVE-2023-52753	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid NULL dereference of t whether assigned timing generator is NULL or not before accessing its funcs to prevent NULL dereference.
CVE-2023-52810	In the Linux kernel, the following vulnerability has been resolved: fs/jfs: Add check for negative db_l2nbperpage l and the minimum legal value should be 0, not negative. In the case of l2nbperpage being negative, an error will occ Syzbot reported this bug: UBSAN: shift-out-of-bounds in fs/jfs/jfs_dmap.c:799:12 shift exponent -16777216 is neg
CVE-2023-52827	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix possible out-of-bound read in a from HTT message and could be an unexpected value in case errors happen, so add validation before using to avoid message iteration and parsing. The same issue also applies to ppdu_info->ppdu_stats.common.num_users, so valid code review. Compile test only.
CVE-2023-52844	In the Linux kernel, the following vulnerability has been resolved: media: vidtv: psi: Add check for kstrdup Add ch return the error if it fails in order to avoid NULL pointer dereference.
CVE-2023-52858	In the Linux kernel, the following vulnerability has been resolved: clk: mediatek: clk-mt7629: Add check for mtk_ value of mtk_alloc_clk_data() in order to avoid NULL pointer dereference.
CVE-2023-52869	In the Linux kernel, the following vulnerability has been resolved: pstore/platform: Add check for kstrdup Add che the error if it fails in order to avoid NULL pointer dereference.
CVE-2023-6176	A null pointer dereference flaw was found in the Linux kernel API for the cryptographic algorithm scatterwalk func constructs a malicious packet with specific socket configuration, which could allow a local user to crash the system
CVE-2023-6240	A Marvin vulnerability side-channel leakage was found in the RSA decryption operation in the Linux Kernel. This decrypt ciphertexts or forge signatures, limiting the services that use that private key.
CVE-2023-6356	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to s using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver and causing
CVE-2023-6535	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to s using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver, causing kern
CVE-2023-6536	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to s using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver, causing kern
CVE-2023-6546	A race condition was found in the GSM 0710 tty multiplexor in the Linux kernel. This issue occurs when two threa the same tty file descriptor with the gsm line discipline enabled, and can lead to a use-after-free problem on a struct could allow a local unprivileged user to escalate their privileges on the system.
CVE-2023-6606	An out-of-bounds read vulnerability was found in smbCalcSize in fs/smb/client/netmisc.c in the Linux Kernel. This the system or leak internal kernel information.
CVE-2023-6915	A Null pointer dereference problem was found in ida_free in lib/idr.c in the Linux Kernel. This issue may allow an service problem due to a missing check at a function return.
CVE-2023-6918	A flaw was found in the libssh implements abstract layer for message digest (MD) operations implemented by differ values from these were not properly checked, which could cause low-memory situations failures, NULL dereference memory as an input for the KDF. In this case, non-matching keys will result in decryption/integrity failures, termin
CVE-2023-7192	A memory leak problem was found in ctnetlink_create_contrack in net/netfilter/nf_contrack_netlink.c in the Lin attacker with CAP_NET_ADMIN privileges to cause a denial of service (DoS) attack due to a refcount overflow.
CVE-2024-0193	A use-after-free flaw was found in the netfilter subsystem of the Linux kernel. If the catchall element is garbage-co element can be deactivated twice. This can cause a use-after-free issue on an NFT_CHAIN object or NFT_OBJECT with CAP_NET_ADMIN capability to escalate their privileges on the system.
CVE-2024-0775	A use-after-free flaw was found in the __ext4_remount in fs/ext4/super.c in ext4 in the Linux kernel. This flaw allo problem while freeing the old quota file names before a potential failure, leading to a use-after-free.
CVE-2024-21803	Use After Free vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (bluetooth modules) allows Local I associated with program files https://gitee.com/anolis/cloud-kernel/blob/devel-5.10/net/bluetooth/af_bluetooth.C . rc2 before v6.8-rc1.
CVE-2024-22189	quic-go is an implementation of the QUIC protocol in Go. Prior to version 0.42.0, an attacker can cause its peer to a number of `NEW_CONNECTION_ID` frames that retire old connection IDs. The receiver is supposed to respond `RETIRE_CONNECTION_ID` frame. The attacker can prevent the receiver from sending out (the vast majority of frames by collapsing the peers congestion window (by selectively acknowledging received packets) and by manipu 0.42.0 contains a patch for the issue. No known workarounds are available.
CVE-2024-22257	In Spring Security, versions 5.7.x prior to 5.7.12, 5.8.x prior to 5.8.11, versions 6.0.x prior to 6.0.9, versions 6.1.x p application is possible vulnerable to broken access control when it directly uses the AuthenticatedVoter#vote passin
CVE-2024-22386	A race condition was found in the Linux kernel's drm/exynos device driver in ~\$exynos_drm_crtc_atomic_disable(dereference issue, possibly leading to a kernel panic or denial of service issue.

CVE-2024-23342	The `ecdsa` PyPI package is a pure Python implementation of ECC (Elliptic Curve Cryptography) with support for ECDSA (Elliptic Curve Digital Signature Algorithm), EdDSA (Edwards-curve Digital Signature Algorithm) and ECDH (Elliptic Curve Diffie-Hellman). Verminerva attack. As of time of publication, no known patched version exists.
CVE-2024-24864	A race condition was found in the Linux kernel's media/dvb-core in dvbdmx_write()→ffunction. This can result in a kernel panic or denial of service issue.
CVE-2024-26583	In the Linux kernel, the following vulnerability has been resolved: tls: fix race between async notify and socket close (recvmsg/sendmsg) may exit as soon as the async crypto handler calls complete() so any code past that point risks to be executed without proper locking and extra flags altogether. Have the main thread hold an extra reference, this way we can depend solely on the completion of the async crypto handler. Don't futz with reiniting the completion, either, we are now tightly controlling when completion fires.
CVE-2024-26583	In the Linux kernel, the following vulnerability has been resolved: tls: fix race between async notify and socket close (recvmsg/sendmsg) may exit as soon as the async crypto handler calls complete() so any code past that point risks to be executed without proper locking and extra flags altogether. Have the main thread hold an extra reference, this way we can depend solely on the completion of the async crypto handler. Don't futz with reiniting the completion, either, we are now tightly controlling when completion fires.
CVE-2024-26584	In the Linux kernel, the following vulnerability has been resolved: net: tls: handle backlogging of crypto requests. Since the CRYPTO_TFM_REQ_MAY_BACKLOG flag on our requests to the crypto API, crypto_aead_{encrypt,decrypt}() can be called in parallel instead of -EINPROGRESS in valid situations. For example, when the cryptd queue for AESNI is full (easy to trigger by running cryptd.cryptd_max_cpu_qlen), requests will be enqueued to the backlog but still processed. In that case, the async crypto handler will first with err == -EINPROGRESS, which it seems we can just ignore, then with err == 0. Compared to Sabrina's original patch, this patch uses tls_*crypt_async_wait() helpers and converts the EBUSY to EINPROGRESS to avoid having to modify all the error handling code.
CVE-2024-26585	In the Linux kernel, the following vulnerability has been resolved: tls: fix race between tx work scheduling and socket close (recvmsg/sendmsg) may exit as soon as the async crypto handler calls complete(). Reorder scheduling of the async crypto handler. This seems more logical in the first place, as it's the inverse order of what the submitting thread will do.
CVE-2024-26800	In the Linux kernel, the following vulnerability has been resolved: tls: fix use-after-free on failed backlog decryption. When a request is added to the backlog and crypto_aead_decrypt returns -EBUSY, tls_do_decryption will wait until all async decryptions have completed. When tls_do_decryption will return -EBADMSG and tls_decrypt_sg jumps to the error path, releasing all the pages. But the async crypto handler will call back, and have already been released by tls_decrypt_done. The only true async case is when crypto_aead_decrypt returns -EBADMSG, we already waited so we can tell tls_sw_recvmsg that the data is available for immediate copy, but we need to notify the async crypto handler (flag) that the memory has already been released.
CVE-2024-26811	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate payload size in ipc response. If a client sends a large payload to ksmbd, ksmbd.mountd can return invalid ipc response to ksmbd kernel server. ksmbd should validate payload size of ipc response to avoid overrun or slab-out-of-bounds. This patch validate 3 ipc response that has payload.
CVE-2024-26841	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Update cpu_sibling_map when disabling nonboot CPUs by defining & calling clear_cpu_sibling_map(), otherwise we get a warning: label: negative count! WARNING: CPU: 6 PID: 45 at kernel/jump_label.c:263 __static_key_slow_dec_cpuslocked+0x10/0x100 CPU: 6 Not tainted 6.8.0-rc5+ #1340 pc 90000000004c302c ra 90000000004c302c tp 900000001005bcb000 sp 9000000000224c278 a2 900000001005bfb58 a3 9000000000224c280 a4 9000000000224c278 a5 900000001005bfb50 a6 9000000000224c278 a7 9000000000224c278 a8 9000000000224c278 a9 9000000000224c278 aa 9000000000224c278 ab 9000000000224c278 ac 9000000000224c278 ad 9000000000224c278 ae 9000000000224c278 af 9000000000224c278 b0 9000000000224c278 b1 9000000000224c278 b2 9000000000224c278 b3 9000000000224c278 b4 9000000000224c278 b5 9000000000224c278 b6 9000000000224c278 b7 9000000000224c278 b8 9000000000224c278 b9 9000000000224c278 ba 9000000000224c278 bb 9000000000224c278 bc 9000000000224c278 bd 9000000000224c278 be 9000000000224c278 bf 9000000000224c278 c0 9000000000224c278 c1 9000000000224c278 c2 9000000000224c278 c3 9000000000224c278 c4 9000000000224c278 c5 9000000000224c278 c6 9000000000224c278 c7 9000000000224c278 c8 9000000000224c278 c9 9000000000224c278 ca 9000000000224c278 cb 9000000000224c278 cc 9000000000224c278 cd 9000000000224c278 ce 9000000000224c278 cf 9000000000224c278 d0 9000000000224c278 d1 9000000000224c278 d2 9000000000224c278 d3 9000000000224c278 d4 9000000000224c278 d5 9000000000224c278 d6 9000000000224c278 d7 9000000000224c278 d8 9000000000224c278 d9 9000000000224c278 da 9000000000224c278 db 9000000000224c278 dc 9000000000224c278 dd 9000000000224c278 de 9000000000224c278 df 9000000000224c278 e0 9000000000224c278 e1 9000000000224c278 e2 9000000000224c278 e3 9000000000224c278 e4 9000000000224c278 e5 9000000000224c278 e6 9000000000224c278 e7 9000000000224c278 e8 9000000000224c278 e9 9000000000224c278 ea 9000000000224c278 eb 9000000000224c278 ec 9000000000224c278 ed 9000000000224c278 ee 9000000000224c278 ef 9000000000224c278 f0 9000000000224c278 f1 9000000000224c278 f2 9000000000224c278 f3 9000000000224c278 f4 9000000000224c278 f5 9000000000224c278 f6 9000000000224c278 f7 9000000000224c278 f8 9000000000224c278 f9 9000000000224c278 fa 9000000000224c278 fb 9000000000224c278 fc 9000000000224c278 fd 9000000000224c278 fe 9000000000224c278 ff 9000000000224c278 00 9000000000224c278 01 9000000000224c278 02 9000000000224c278 03 9000000000224c278 04 9000000000224c278 05 9000000000224c278 06 9000000000224c278 07 9000000000224c278 08 9000000000224c278 09 9000000000224c278 0a 9000000000224c278 0b 9000000000224c278 0c 9000000000224c278 0d 9000000000224c278 0e 9000000000224c278 0f 9000000000224c278 10 9000000000224c278 11 9000000000224c278 12 9000000000224c278 13 9000000000224c278 14 9000000000224c278 15 9000000000224c278 16 9000000000224c278 17 9000000000224c278 18 9000000000224c278 19 9000000000224c278 1a 9000000000224c278 1b 9000000000224c278 1c 9000000000224c278 1d 9000000000224c278 1e 9000000000224c278 1f 9000000000224c278 20 9000000000224c278 21 9000000000224c278 22 9000000000224c278 23 9000000000224c278 24 9000000000224c278 25 9000000000224c278 26 9000000000224c278 27 9000000000224c278 28 9000000000224c278 29 9000000000224c278 2a 9000000000224c278 2b 9000000000224c278 2c 9000000000224c278 2d 9000000000224c278 2e 9000000000224c278 2f 9000000000224c278 30 9000000000224c278 31 9000000000224c278 32 9000000000224c278 33 9000000000224c278 34 9000000000224c278 35 9000000000224c278 36 9000000000224c278 37 9000000000224c278 38 9000000000224c278 39 9000000000224c278 3a 9000000000224c278 3b 9000000000224c278 3c 9000000000224c278 3d 9000000000224c278 3e 9000000000224c278 3f 9000000000224c278 40 9000000000224c278 41 9000000000224c278 42 9000000000224c278 43 9000000000224c278 44 9000000000224c278 45 9000000000224c278 46 9000000000224c278 47 9000000000224c278 48 9000000000224c278 49 9000000000224c278 4a 9000000000224c278 4b 9000000000224c278 4c 9000000000224c278 4d 9000000000224c278 4e 9000000000224c278 4f 9000000000224c278 50 9000000000224c278 51 9000000000224c278 52 9000000000224c278 53 9000000000224c278 54 9000000000224c278 55 9000000000224c278 56 9000000000224c278 57 9000000000224c278 58 9000000000224c278 59 9000000000224c278 5a 9000000000224c278 5b 9000000000224c278 5c 9000000000224c278 5d 9000000000224c278 5e 9000000000224c278 5f 9000000000224c278 60 9000000000224c278 61 9000000000224c278 62 9000000000224c278 63 9000000000224c278 64 9000000000224c278 65 9000000000224c278 66 9000000000224c278 67 9000000000224c278 68 9000000000224c278 69 9000000000224c278 6a 9000000000224c278 6b 9000000000224c278 6c 9000000000224c278 6d 9000000000224c278 6e 9000000000224c278 6f 9000000000224c278 70 9000000000224c278 71 9000000000224c278 72 9000000000224c278 73 9000000000224c278 74 9000000000224c278 75 9000000000224c278 76 9000000000224c278 77 9000000000224c278 78 9000000000224c278 79 9000000000224c278 7a 9000000000224c278 7b 9000000000224c278 7c 9000000000224c278 7d 9000000000224c278 7e 9000000000224c278 7f 9000000000224c278 80 9000000000224c278 81 9000000000224c278 82 9000000000224c278 83 9000000000224c278 84 9000000000224c278 85 9000000000224c278 86 9000000000224c278 87 9000000000224c278 88 9000000000224c278 89 9000000000224c278 8a 9000000000224c278 8b 9000000000224c278 8c 9000000000224c278 8d 9000000000224c278 8e 9000000000224c278 8f 9000000000224c278 90 9000000000224c278 91 9000000000224c278 92 9000000000224c278 93 9000000000224c278 94 9000000000224c278 95 9000000000224c278 96 9000000000224c278 97 9000000000224c278 98 9000000000224c278 99 9000000000224c278 9a 9000000000224c278 9b 9000000000224c278 9c 9000000000224c278 9d 9000000000224c278 9e 9000000000224c278 9f 9000000000224c278 a0 9000000000224c278 a1 9000000000224c278 a2 9000000000224c278 a3 9000000000224c278 a4 9000000000224c278 a5 9000000000224c278 a6 9000000000224c278 a7 9000000000224c278 a8 9000000000224c278 a9 9000000000224c278 aa 9000000000224c278 ab 9000000000224c278 ac 9000000000224c278 ad 9000000000224c278 ae 9000000000224c278 af 9000000000224c278 b0 9000000000224c278 b1 9000000000224c278 b2 9000000000224c278 b3 9000000000224c278 b4 9000000000224c278 b5 9000000000224c278 b6 9000000000224c278 b7 9000000000224c278 b8 9000000000224c278 b9 9000000000224c278 ba 9000000000224c278 bb 9000000000224c278 bc 9000000000224c278 bd 9000000000224c278 be 9000000000224c278 bf 9000000000224c278 c0 9000000000224c278 c1 9000000000224c278 c2 9000000000224c278 c3 9000000000224c278 c4 9000000000224c278 c5 9000000000224c278 c6 9000000000224c278 c7 9000000000224c278 c8 9000000000224c278 c9 9000000000224c278 ca 9000000000224c278 cb 9000000000224c278 cc 9000000000224c278 cd 9000000000224c278 ce 9000000000224c278 cf 9000000000224c278 d0 9000000000224c278 d1 9000000000224c278 d2 9000000000224c278 d3 9000000000224c278 d4 9000000000224c278 d5 9000000000224c278 d6 9000000000224c278 d7 9000000000224c278 d8 9000000000224c278 d9 9000000000224c278 da 9000000000224c278 db 9000000000224c278 dc 9000000000224c278 dd 9000000000224c278 de 9000000000224c278 df 9000000000224c278 e0 9000000000224c278 e1 9000000000224c278 e2 9000000000224c278 e3 9000000000224c278 e4 9000000000224c278 e5 9000000000224c278 e6 9000000000224c278 e7 9000000000224c278 e8 9000000000224c278 e9 9000000000224c278 ea 9000000000224c278 eb 9000000000224c278 ec 9000000000224c278 ed 9000000000224c278 ee 9000000000224c278 ef 9000000000224c278 f0 9000000000224c278 f1 9000000000224c278 f2 9000000000224c278 f3 9000000000224c278 f4 9000000000224c278 f5 9000000000224c278 f6 9000000000224c278 f7 9000000000224c278 f8 9000000000224c278 f9 9000000000224c278 fa 9000000000224c278 fb 9000000000224c278 fc 9000000000224c278 fd 9000000000224c278 fe 9000000000224c278 ff 9000000000224c278 00 9000000000224c278 01 9000000000224c278 02 9000000000224c278 03 9000000000224c278 04 9000000000224c278 05 9000000000224c278 06 9000000000224c278 07 9000000000224c278 08 9000000000224c278 09 9000000000224c278 0a 9000000000224c278 0b 9000000000224c278 0c 9000000000224c278 0d 9000000000224c278 0e 9000000000224c278 0f 9000000000224c278 10 9000000000224c278 11 9000000000224c278 12 9000000000224c278 13 9000000000224c278 14 9000000000224c278 15 9000000000224c278 16 9000000000224c278 17 9000000000224c278 18 9000000000224c278 19 9000000000224c278 1a 9000000000224c278 1b 9000000000224c278 1c 9000000000224c278 1d 9000000000224c278 1e 9000000000224c278 1f 9000000000224c278 20 9000000000224c278 21 9000000000224c278 22 9000000000224c278 23 9000000000224c278 24 9000000000224c278 25 9000000000224c278 26 9000000000224c278 27 9000000000224c278 28 9000000000224c278 29 9000000000224c278 2a 9000000000224c278 2b 9000000000224c278 2c 9000000000224c278 2d 9000000000224c278 2e 9000000000224c278 2f 9000000000224c278 30 9000000000224c278 31 9000000000224c278 32 9000000000224c278 33 9000000000224c278 34 9000000000224c278 35 9000000000224c278 36 9000000000224c278 37 9000000000224c278 38 9000000000224c278 39 9000000000224c278 3a 9000000000224c278 3b 9000000000224c278 3c 9000000000224c278 3d 9000000000224c278 3e 9000000000224c278 3f 9000000000224c278 40 9000000000224c278 41 9000000000224c278 42 9000000000224c278 43 9000000000224c278 44 9000000000224c278 45 9000000000224c278 46 9000000000224c278 47 9000000000224c278 48 9000000000224c278 49 9000000000224c278 4a 9000000000224c278 4b 9000000000224c278 4c 9000000000224c278 4d 9000000000224c278 4e 9000000000224c278 4f 9000000000224c278 50 9000000000224c278 51 9000000000224c278 52 9000000000224c278 53 9000000000224c278 54 9000000000224c278 55 9000000000224c278 56 9000000000224c278 57 9000000000224c278 58 9000000000224c278 59 9000000000224c278 5a 9000000000224c278 5b 9000000000224c278 5c 9000000000224c278 5d 9000000000224c278 5e 9000000000224c278 5f 9000000000224c278 60 9000000000224c278 61 9000000000224c278 62 9000000000224c278 63 9000000000224c278 64 9000000000224c278 65 9000000000224c278 66 9000000000224c278 67 9000000000224c278 68 9000000000224c278 69 9000000000224c278 6a 9000000000224c278 6b 9000000000224c278 6c 9000000000224c278 6d 9000000000224c278 6e 9000000000224c278 6f 9000000000224c278 70 9000000000224c278 71 9000000000224c278 72 9000000000224c278 73 9000000000224c278 74 9000000000224c278 75 9000000000224c278 76 9000000000224c278 77 9000000000224c278 78 9000000000224c278 79 9000000000224c278 7a 9000000000224c278 7b 9000000000224c278 7c 9000000000224c278 7d 9000000000224c278 7e 9000000000224c278 7f 9000000000224c278 80 9000000000224c278 81 9000000000224c278 82 9000000000224c278 83 9000000000224c278 84 9000000000224c278 85 9000000000224c278 86 9000000000224c278 87 9000000000224c278 88 9000000000224c278 89 9000000000224c278 8a 9000000000224c278 8b 9000000000224c278 8c 9000000000224c278 8d 9000000000224c278 8e 9000000000224c278 8f 9000000000224c278 90 9000000000224c278 91 9000000000224c278 92 9000000000224c278 93 9000000000224c278 94 9000000000224c278 95 9000000000224c278 96 9000000000224c278 97 9000000000224c278 98 9000000000224c278 99 9000000000224c278 9a 9000000000224c278 9b 9000000000224c278 9c 9000000000224c278 9d 9000000000224c278 9e 9000000000224c278 9f 9000000000224c278 a0 9000000000224c278 a1 9000000000224c278 a2 9000000000224c278 a3 9000000000224c278 a4 9000000000224c278 a5 9000000000224c278 a6 9000000000224c278 a7 9000000000224c278 a8 9000000000224c278 a9 9000000000224c278 aa 9000000000224c278 ab 9000000000224c278 ac 9000000000224c278 ad 9000000000224c278 ae 9000000000224c278 af 9000000000224c278 b0 9000000000224c278 b1 9000000000224c278 b2 9000000000224c278 b3 9000000000224c278 b4 9000000000224c278 b5 9000000000224c278 b6 9000000000224c278 b7 9000000000224c278 b8 9000000000224c278 b9 9000000000224c278 ba 9000000000224c278 bb 9000000000224c278 bc 9000000000224c278 bd 9000000000224c278 be 9000000000224c2

CVE-2024-26893	<p>In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Fix double free in SMC transport code tears down a channel, it calls the chan_free callback function, defined by each transport. Since multiple protocol member, chan_free() might want to clean up the same member multiple times within the given SCMI transport implementation. This will lead to a NULL pointer dereference at the second time: scm_i_protocol scm_i_dev.1: Enabled po arm-scmi firmware:scmi: SCMI Notifications - Core Enabled. arm-scmi firmware:scmi: unable to communicate NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000096000004 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 user pgtable: 4k pages, [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000000 CPU: 4 PID: 1 Comm: swapper/0 Not tainted 6.7.0-rc2-00124-g455ef3d016c9-dirty #793 Hardware name: FVP daif +PAN -UAO -TCO +DIT -SSBS BTYP= pc : smc_chan_free+0x3c/0x6c lr : smc_chan_free+0x3c/0x6c idr_for_each+0x68/0xf8 scm_i_cleanup_channels.isra.0+0x2c/0x58 scm_i_probe+0x434/0x734 platform_probe __driver_probe_device+0x78/0x12c driver_probe_device+0x3c/0x118 __driver_attach+0x74/0x128 bus_for +0x24/0x30 bus_add_driver+0xe4/0x1e8 driver_register+0x60/0x128 __platform_driver_register+0x28/0x34 +0x78/0x33c kernel_init_freeable+0x2b8/0x51c kernel_init+0x24/0x130 ret_from_fork+0x10/0x20 Code: f00 (b9400280) ---[end trace 0000000000000000]--- Simply check for the struct pointer being NULL before trying to free it. This was found when a transport doesn't really work (for instance no SMC service), the probe routines then tries to</p>
CVE-2024-26896	<p>In the Linux kernel, the following vulnerability has been resolved: wifi: wfx: fix memory leak when starting AP K object 0xd73d1180 (size 184): comm "wpa_supplicant", pid 1559, jiffies 13006305 (age 964.245s) hex dump (first 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 00 01 00 00 00 00 backtrace: [<5ca11420>] kmalloc_reserve.constprop.0+0x30/0x74 [a2c61343] __alloc_skb+0xa0/0x170 [fb8a5e38] __ieee80211_beacon_get+0x54/0x18c [mac80211] [<41e25cc3>] wfx_start_ap+0xc8/0x234 [wfx] [<93a70356>] [mac80211] [<a4a661cd>] nl80211_start_ap+0x76c/0x9e0 [cfg80211] [<47bd8b68>] genl_rcv_msg+0x198/0x378 +0xd0/0x130 [<6b7c977a>] genl_rcv+0x34/0x44 [<66b2d04d>] netlink_unicast+0x1b4/0x258 [<f965b9b6>] netlink_sendmsg+0x1e0/0x274 [<d2b5212d>] __sys_sendmsg+0x80/0xb4 [<69954f45>] __sys_sendmsg+0x64 (size 1024): comm "wpa_supplicant", pid 1559, jiffies 13006305 (age 964.246s) hex dump (first 32 bytes): 00 00 00 00 00 10 00 07 40 00 backtrace: [<9a993714>] kmalloc_reserve.constprop.0+0x30/0x74 [a2c61343] __alloc_skb+0xa0/0x170 [fb8a5e38] __ieee80211_beacon_get+0x54/0x18c [mac80211] [<7acd02d>] ieee80211_beacon_get+0x54/0x18c [mac80211] [<93a70356>] wfx_start_ap+0xc8/0x234 [wfx] [<93a70356>] ieee80211_start_ap+0x76c/0x9e0 [cfg80211] [<a4a661cd>] nl80211_start_ap+0x76c/0x9e0 [cfg80211] [<47bd8b68>] genl_rcv_msg+0x198/0x378 [<453ef796>] netlink_rcv_skb+0xd0/0x130 [<6b7c977a>] genl_rcv+0x34/0x44 [<66b2d04d>] netlink_unicast+0x1b4/0x258 [<f965b9b6>] netlink_sendmsg+0x1e0/0x274 [<aadb8231>] __sys_sendmsg+0x1e0/0x274 [<d2b5212d>] __sys_sendmsg kernel is build optimized, it seems the stack is not accurate. It appears the issue is related to wfx_set_mfp_ap(). The allocated by ieee80211_beacon_get() is never released. Fixing this leak makes kmemleak happy.</p>
CVE-2024-26907	<p>In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix fortify source warning while [cut here]----- memcpy: detected field-spanning write (size 56) of single field "eseg->inline_hdr.start" at /var/build/drivers/infiniband/hw/mlx5/wr.c:131 (size 2) WARNING: CPU: 0 PID: 293779 at /var/lib/dkms/mlnx-ofed-kernel-5.0-1.0/build/drivers/infiniband/hw/mlx5/wr.c:131 mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] Modules linked in: 8021q garp mrp stp llc rdma_ib_ibipoib(OE) ib_cm(OE) ib_umad(OE) mlx5_ib(OE) ib_uverbs(OE) ib_core(OE) mlx5_core(OE) pci_hyperv_intf mlxfw(OE) psample nft_fib_inet nft_fib_ipv6 nft_fib_ipv4 nft_fib_nat nft_fib_reject_inet nft_reject_ipv4 nft_reject_ipv6 nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 ip_set nf_tables liberc32c nfnetlink mst_pciconf(OE) knem(OE) vfio_vfio iommufd irqbypass fuse nfsv3 nfs fscache netfs xfrm_user xfrm_algo ipmi_devintf ipmi_msghandler binfmt_polyval cmlmulni polyval_generic ghash_cmlmulni_intel sha512_ssse3 snd_pcsp aesni_intel crypto_simd cryptd snd_input_leds serio_raw evbug nfsd auth_rpcgss nfs_acl lockd grace sch_fq_codel sunrpc drm_efi_pstore ip_tables x_tables net_failover failover floppy [last unloaded: mlx_compat(OE)] CPU: 0 PID: 293779 Comm: ssh Tainted: G OE 6.2. Hardware name: Red Hat KVM, BIOS 0.5.1 01/01/2011 RIP: 0010:mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] a0 b9 02 00 00 00 48 c7 c2 10 5b fd c0 48 c7 c7 80 5b fd c0 c6 05 57 0c 03 00 01 e8 95 4d 93 da <0f> 0b 44 8b 4d ff ff 41 0f b7 RSP: 0018:ffff5b48478b570 EFLAGS: 00010046 RAX: 0000000000000000 RBX: 0000000000000000 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff5b48478b628 R08: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffff5b48478b5e8 R13: ffff963a3c609b5e R14: ffff9639c FS: 00007fc03b444c80(0000) GS:ffff963a3dc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 0000556f46bdf000 CR3: 0000000006ac6003 CR4: 00000000003706f0 DR0: 0000000000000000 DR1: 0000000000000000 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? show_regs+0x72/0x [mlx5_ib] ? __warn+0x8d/0x160 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? report_bug+0x1bb/0x1d0 ? ha +0x19/0x80 ? asm_exc_invalid_op+0x1b/0x20 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] mlx5_ib_post_send+0x2ec/0x770 [ib_ipoib] ipoib_start_xmit+0x5a0/0x770 [ib_ipoib] dev_hard_start_xmit+0x8e/0x1e0 ? validate_xr +0x116/0x3a0 __dev_xmit_skb+0x1fd/0x580 __dev_queue_xmit+0x284/0x6b0 ? __raw_spin_unlock_irq+0xe/0x5f push_pseudo_header+0x17/0x40 [ib_ipoib] neigh_connected_output+0xcd/0x110 ip_finish_output2+0x179/0x480 __ip_finish_output+0xc3/0x190 ip_finish_output+0x2e/0xf0 ip_output+0x78/0x110 ? __pfx_ip_finish_output+0x1 __ip_queue_xmit+0x18a/0x460 ip_queue_xmit+0x15/0x30 __tcp_transmit_skb+0x914/0x9c0 tcp_write_xmit+0x5 tcp_sendmsg_locked+0x2e1/0xac0 tcp_sendmsg+0x2d/0x50 inet_sendmsg+0x43/0x90 sock_sendmsg+0x68/0x80 +0x326/0x3c0 ksys_write+0xbd/0xf0 ? do_syscall_64+0x69/0x90 __x64_sys_write+0x19/0x30 do_syscall_---trun</p>
CVE-2024-26913	<p>In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix dcn35 8k30 Underflow/Corruption for pipe split policy determination and cause Underflow/Corruption issue. [how] Add the odm calculation.</p>
CVE-2024-26914	<p>In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: fix incorrect mpc_combine array size, while MAX_PLANES is per asic. The mpc_combine is an array that records all the planes per asic. Therefore array size. Using MAX_SURFACES causes array overflow when there are more than 3 planes. [how] Use the MAX</p>

CVE-2024-26952	In the Linux kernel, the following vulnerability has been resolved: ksmdbd: fix potencial out-of-bounds when buffer bounds when buffer offset fields of a few requests is invalid. This patch set the minimum value of buffer offset field
CVE-2024-27034	In the Linux kernel, the following vulnerability has been resolved: f2fs: compress: fix to cover normal cluster write compressed cluster w/ normal cluster, we should not unlock cp_rwsem during f2fs_write_raw_pages(), otherwise d persisted before CP & SPOR, due to cluster metadata wasn't updated atomically.
CVE-2024-27035	In the Linux kernel, the following vulnerability has been resolved: f2fs: compress: fix to guarantee persisting comp compressed cluster is not persisted with metadata during checkpoint, after SPOR, the data may be corrupted, let's g checkpoint.
CVE-2024-27389	In the Linux kernel, the following vulnerability has been resolved: pstore: inode: Only d_invalidate() is needed Un records in pstorefs would trigger the dput() double-drop warning: WARNING: CPU: 0 PID: 2569 at fs/dcache.c:76 of d_drop()/dput() (as mentioned in Documentation/filesystems/vfs.rst) isn't the right approach here, and leads to th Use d_invalidate() and update the code to not bother checking for error codes that can never happen. ---
CVE-2024-27393	In the Linux kernel, the following vulnerability has been resolved: xen-netfront: Add missing skb_mark_for_recycl introduced later than fixes tag in commit 6a5bcd84e886 ("page_pool: Allow drivers to hint on SKB recycling"). It to page_pool_release_page() between v5.9 to v5.14, after which is should have used skb_mark_for_recycle(). Since were removed (in commit 535b9c61bdef ("net: page_pool: hide page_pool_release_page()") and remaining callers branch 'net-page_pool-remove-page_pool_release_page')). This leak became visible in v6.8 via commit dba1b8a7 memory leaks").
CVE-2024-28849	follow-redirects is an open source, drop-in replacement for Node's `http` and `https` modules that automatically fol follow-redirects only clears authorization header during cross-domain redirect, but keep the proxy-authentication h vulnerability may lead to credentials leak, but has been addressed in version 1.15.6. Users are advised to upgrade. T vulnerability.
CVE-2024-35785	In the Linux kernel, the following vulnerability has been resolved: tee: optee: Fix kernel panic caused by incorrect to register devices on the TEE bus has a bug leading to kernel panic as follows: [15.398930] Unable to handle kern ffff07ed00626d7c [15.406913] Mem abort info: [15.409722] ESR = 0x0000000096000005 [15.413490] EC = 0x [15.418814] SET = 0, FnV = 0 [15.421878] EA = 0, S1PTW = 0 [15.425031] FSC = 0x05: level 1 translation faul ISV = 0, ISS = 0x00000005, ISS2 = 0x00000000 [15.438310] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [15.44 = 0, Xs = 0 [15.448697] swapper pgtable: 4k pages, 48-bit VAs, pgdp=00000000d9e3e000 [15.455413] [ffff07ed p4d=1800000bffd9003, pud=0000000000000000 [15.464146] Internal error: Oops: 0000000096000005 [#1] PRE optee: Fix supplicant based device enumeration") lead to the introduction of this bug. So fix it appropriately.
CVE-2024-35796	In the Linux kernel, the following vulnerability has been resolved: net: ll_temac: platform_get_resource replaced b platform_get_resource was replaced with devm_platform_ioremap_resource_byname and is called using 0 as name platform_get_resource_byname in the call stack, where it causes a null pointer in strcmp. if (type == resource_type have been replaced with devm_platform_ioremap_resource.
CVE-2024-35811	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: Fix use-after-free bug in brcmf patch of CVE-2023-47233 : https://nvd.nist.gov/vuln/detail/CVE-2023-47233 In brcm80211 driver, it starts with the timeout worker: ->brcmf_usb_probe ->brcmf_usb_probe_cb ->brcmf_attach ->brcmf_bus_started ->brcmf_cfg80211 ->INIT_WORK(&cfg->escan_timeout_work, brcmf_cfg80211_escan_timeout_worker); If we disconnect the USB to make cleanup. The invoking chain is : brcmf_usb_disconnect ->brcmf_usb_disconnect_cb ->brcmf_detach ->br the timeout woker may still be running. This will cause a use-after-free bug on cfg in brcmf_cfg80211_escan_timeo canceling the worker in brcmf_cfg80211_detach. [arend.vanspriel@broadcom.com: keep timer delete as is and can
CVE-2024-35818	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Define the __io_aw() hook as mmio ("drivers: Remove explicit invocations of mmiowb()") remove all mmiowb() in drivers, but it says: "NOTE: mmiowb in conjunction with spin_unlock(). However, pairing each mmiowb() removal in this patch with the corresponding so there is a small chance that this change may regress any drivers incorrectly relying on mmiowb() to order MMIO synchronisation." The mmio in radeon_ring_commit() is protected by a mutex rather than a spinlock, but in the mu We can add mmiowb() calls in the radeon driver but the maintainer says he doesn't like such a workaround, and rade protected mmio. So we should extend the mmiowb tracking system from spinlock to mutex, and maybe other locki prone, so we solve it in the architectural code, by simply defining the __io_aw() hook as mmiowb(). And we no lon so use the generic definition. Without this, we get such an error when run 'glxgears' on weak ordering architectures ring 0 stalled for more than 10324msec radeon 0000:04:00.0: ring 3 stalled for more than 10240msec radeon 0000: 0x000000000001f412 last fence id 0x000000000001f414 on ring 3) radeon 0000:04:00.0: GPU lockup (current fer 0x000000000000f941 on ring 0) radeon 0000:04:00.0: scheduling IB failed (-35). [drm:radeon_gem_va_ioctl [rade (-35) radeon 0000:04:00.0: scheduling IB failed (-35). [drm:radeon_gem_va_ioctl [radeon]] *ERROR* Couldn't up scheduling IB failed (-35). [drm:radeon_gem_va_ioctl [radeon]] *ERROR* Couldn't update BO_VA (-35) radeon [drm:radeon_gem_va_ioctl [radeon]] *ERROR* Couldn't update BO_VA (-35) radeon 0000:04:00.0: scheduling IB [radeon]] *ERROR* Couldn't update BO_VA (-35) radeon 0000:04:00.0: scheduling IB failed (-35). [drm:radeon update BO_VA (-35) radeon 0000:04:00.0: scheduling IB failed (-35). [drm:radeon_gem_va_ioctl [radeon]] *ERR
CVE-2024-35829	In the Linux kernel, the following vulnerability has been resolved: drm/lima: fix a memleak in lima_heap_alloc W need to be deallocated, or there will be memleaks.

CVE-2024-35833	In the Linux kernel, the following vulnerability has been resolved: dmaengine: fsl-qdma: Fix a memory leak related to dma_alloc_coherent() is undone neither in the remove function, nor in the error handling path of fsl_qdma_probe() issues.
CVE-2024-35835	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: fix a double-free in arfs_create_group arfs_create_groups will free ft->g and return an error. However, arfs_create_table, the only caller of arfs_create_group, calls mlx5e_destroy_flow_table, in which the ft->g will be freed again.
CVE-2024-35844	In the Linux kernel, the following vulnerability has been resolved: f2fs: compress: fix reserve_cblocks counting error one direct_node, performing the following operations will cause the file to be unrepairable: unisoc # ./f2fs_io comp dev/block/dm-48 112G 112G 1.2M 100% /data unisoc # ./f2fs_io release_cblocks test.apk 924 unisoc # df -h grep 100% /data unisoc # dd if=/dev/random of=file4 bs=1M count=3 3145728 bytes (3.0 M) copied, 0.025 s, 120 M/s unisoc # 112G 112G 1.8M 100% /data unisoc # ./f2fs_io reserve_cblocks test.apk F2FS_IOC_RESERVE_COMPRESS_BLOCK unisoc # reboot unisoc # df -h grep dm-48 /dev/block/dm-48 112G 112G 11M 100% /data unisoc # ./f2fs_io reserve_cblocks test.apk After returning to -ENOSPC, reserved_blocks += ret will not be executed. As a result, the reserve_cblocks does not reflect the real number of reserved blocks. Therefore, fsck cannot be set to repair the file. After this patch, the fsck flag will be set by grep dm-48 /dev/block/dm-48 112G 112G 1.8M 100% /data unisoc # ./f2fs_io reserve_cblocks test.apk F2FS_IOC_RESERVE_COMPRESS_BLOCK No space left on device adb reboot then fsck will be executed unisoc # df -h grep dm-48 /dev/block/dm-48 112G 112G 1.8M 100% /data unisoc # reserve_cblocks test.apk 924
CVE-2024-35845	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: dbg-tlv: ensure NUL termination of string, so we must ensure the string is terminated correctly before using it.
CVE-2024-35879	In the Linux kernel, the following vulnerability has been resolved: of: dynamic: Synchronize of_changeset_destroy sequence: 1) of_platform_depopulate() 2) of_overlay_remove() During the step 1, devices are destroyed and devlink entries are destroyed but __of_changeset_entry_destroy() can raise warnings related to missing of_node_put(): ERROR: n... 2 ... Indeed, during the devlink removals performed at step 1, the removal itself releasing the device (and the attach workqueue and so, it is done asynchronously with respect to function calls. When the warning is present, of_node_get() is called on the workqueue job. In order to be sure that any ongoing devlink removals are done before the of_node destruction, the devlink removals.
CVE-2024-35902	In the Linux kernel, the following vulnerability has been resolved: net/rds: fix possible cp null dereference cp might be NULL null dereference [Simon Horman adds:] Analysis: * cp is a parameter of __rds_rdma_map and is not reassigned. * cp argument to __rds_rdma_map() - rds_get_mr() - rds_get_mr_for_dest * Prior to the code above, the following assignment is indicative, but could itself be unnecessary) trans_private = rs->rs_transport->get_mr(sg, nents, rs, &mr->r_key, cp, args->vec.bytes, need_odp ? ODP_ZEROBASED : ODP_NOT_NEEDED); * The code modified by this patch is get_mr(trans_private) is assigned as per the previous point in this analysis. The only implementation of get_mr that I could find was an ERR_PTR if the conn (4th) argument is NULL. * ret is set to PTR_ERR(trans_private). rds_ib_get_mr can return an ERR_PTR if the conn (4th) argument is NULL. Thus ret may be -ENODEV in which case the code in question will execute. Conclusion: * cp is added; this patch does seem to address a possible bug
CVE-2024-35956	In the Linux kernel, the following vulnerability has been resolved: btrfs: qgroup: fix qgroup prealloc rsv leak in subtree create snapshot and delete subvolume all use btrfs_subvolume_reserve_metadata() to reserve metadata for the change tree, which cannot be mediated in the normal way via start_transaction. When quota groups (squota or qgroups) are of type PREALLOC. Once the operation is associated to a transaction, we convert PREALLOC to PERTRANS, with start_transaction. However, the error paths of these three operations were not implementing this lifecycle correctly. They converted to PERTRANS in a generic cleanup step regardless of errors or whether the operation was fully associated to a transaction occasionally converting this rsv to PERTRANS without calling record_root_in_trans successfully, which meant that the transaction by some other thread, the end of the transaction would not free that root's PERTRANS, leaking it. Ultimately CONFIG_BTRFS_DEBUG builds at umount for the leaked reservation. The fix is to ensure that every qgroup PRERELEASE has properties: 1. any failure before record_root_in_trans is called successfully results in freeing the PREALLOC reservation. If we convert to PERTRANS, and now the transaction owns freeing the reservation. This patch enforces those properties. generic/269 with quotas enabled at mkfs time would fail in ~5-10 runs on my system. With this patch, it ran successfully
CVE-2024-35971	In the Linux kernel, the following vulnerability has been resolved: net: ks8851: Handle softirqs at the end of IRQ thread the thread may call ks8851_rx_pkts() in case there are any packets in the MAC FIFO, which calls netif_rx(). This netif_rx() calls local_bh_disable() and local_bh_enable(). The local_bh_enable() may call do_softirq() to run softirqs in case any action is net_rx_action, which ultimately reaches the driver .start_xmit callback. If that happens, the system hangs. The exit from netdev_start_xmit netdev_start_xmit from dev_hard_start_xmit dev_hard_start_xmit from sch_direct_xmit sch_direct_xmit from __dev_queue_xmit from __neigh_update __neigh_update from neigh_update neigh_update from arp_process.consistent __netif_receive_skb_one_core __netif_receive_skb_one_core from process_backlog process_backlog from __napi_poll from net_rx_action net_rx_action from __do_softirq __do_softirq from call_with_stack call_with_stack from do_softirq __local_bh_enable_ip from netif_rx netif_rx from ks8851_irq from irq_thread fn irq_thread_fn from irq_thread_fn from ret_from_fork The hang happens because ks8851_irq() first locks a spinlock in ks8851_par.c ks8851_lock_irq with that spinlock locked, calls netif_rx(). Once the execution reaches ks8851_start_xmit_par(), it calls ks8851_lock_irq already locked spinlock again, and the hang happens. Move the do_softirq() call outside of the spinlock protected section around the entire spinlock protected section of ks8851_irq() handler. Place local_bh_enable() outside of the spinlock protected section do_softirq() without the ks8851_par.c ks8851_lock_irq spinlock being held, and safely call ks8851_start_xmit_par() with the locked spinlock. Since ks8851_irq() is protected by local_bh_disable()/local_bh_enable() now, replace netif_rx() with local_bh_disable()/local_bh_enable() calls.

CVE-2024-35988	In the Linux kernel, the following vulnerability has been resolved: riscv: Fix TASK_SIZE on 64-bit NOMMU On anywhere in physical RAM. The current definition of TASK_SIZE is wrong if any RAM exists above 4G, causing routines.
CVE-2024-35990	In the Linux kernel, the following vulnerability has been resolved: dma: xilinx_dpdma: Fix locking There are several chan->vchan.lock was not held. Add appropriate locking. This fixes lockdep warnings like [31.077578] ----- WARNING: CPU: 2 PID: 40 at drivers/dma/xilinx/xilinx_dpdma.c:834 xilinx_dpdma_chan_queue_transfer+0x274 linked in: [31.078019] CPU: 2 PID: 40 Comm: kworker/u12:1 Not tainted 6.6.20+ #98 [31.078102] Hardware name: Workqueue: events_unbound deferred_probe_work_func [31.078272] pstate: 600000c5 (nZCv daIF -PAN -UAO) [31.078377] pc : xilinx_dpdma_chan_queue_transfer+0x274/0x5e0 [31.078473] lr : xilinx_dpdma_chan_queue_transfer+0x274/0x5e0 [31.078590] x29: ffffffff083bb2e10 [31.078590] x28: 0000000000000000 x27: ffffffff880165a168 [31.078590] x24: ffffffff880164eab8 x23: ffffffff880164d480 [31.078920] x22: ffffffff880164e988 x21: 00000000 ffffffff082aa3000 x19: ffffffff880164e880 x18: 0000000000000000 [31.079295] x17: 0000000000000000 x16: 0000 [31.079453] x14: 0000000000000000 x13: ffffffff8802263dc0 x12: 0000000000000001 [31.079613] x11: 0001ffcf x9 : 0001ffcf082aa3def [31.079824] x8 : 0001ffcf082aa3dec x7 : 0000000000000000 x6 : 00000000000000516 [31.079984] x5 : ffffffff88003c9c40 x3 : ffffffff00000000 [31.080147] x2 : ffffffff7f8d43000 x1 : 0000000000000000 x0 : 000000000000 xilinx_dpdma_chan_queue_transfer+0x274/0x5e0 [31.080518] xilinx_dpdma_issue_pending+0x11c/0x120 [31.080518] +0x180/0x3ac [31.080712] zynqmp_dpsub_plane_atomic_update+0x11c/0x21c [31.080825] drm_atomic_helper_commit_tail+0x5c/0xb0 [31.081139] commit_tail+0x234/0x294 [31.081246] drm_atomic_helper_commit+0x100/0x140 [31.081477] drm_client_modeset_commit_atomic+0x318/0x384 [31.081634] drm_client_modeset_commit_atomic+0x318/0x384 [31.081634] +0x8c/0x24c [31.081725] drm_client_modeset_commit+0x34/0x5c [31.081812] __drm_fb_helper_restore_fbdev [31.081899] drm_fb_helper_set_par+0x50/0x70 [31.081971] fbcon_init+0x538/0xc48 [31.082047] visual_init+0x0 [31.082047] do_bind_con_driver.isra.0+0x2d0/0x634 [31.082320] do_take_over_console+0x24c/0x33c [31.082429] do_fbcon_fbcon_fb_registered+0x2d0/0x34c [31.082663] register_framebuffer+0x27c/0x38c [31.082767] __drm_fb_helper [31.082939] drm_fb_helper_initial_config+0x50/0x74 [31.083012] drm_fbdev_dma_client_hotplug+0xb8/0x108 [31.083175] +0xa0/0xf4 [31.083195] drm_fbdev_dma_setup+0xb0/0x1cc [31.083293] zynqmp_dpsub_drm_init+0x45c/0x4ef [31.083378] +0x444/0x5e0 [31.083616] platform_probe+0x8c/0x13c [31.083713] really_probe+0x258/0x59c [31.083793] __ [31.083878] driver_probe_device+0x70/0x1c0 [31.083961] __device_attach_driver+0x108/0x1e0 [31.084052] b [31.084125] __device_attach+0x100/0x298 [31.084207] device_initial_probe+0x14/0x20 [31.084292] bus_probe_device [31.084292] deferred_probe_work_func+0x11c/0x180 [31.084451] process_one_work+0x3ac/0x988 [31.084643] worker_thread [31.084643] +0x1bc/0x1c0 [31.084848] ret_from_fork+0x10/0x20 [31.084932] irq event stamp: 64549 [31.084970] hardirqs [31.084970] _raw_spin_unlock_irqrestore+0x80/0x90 [31.085157] ---truncated---
CVE-2024-36008	In the Linux kernel, the following vulnerability has been resolved: ipv4: check for NULL idev in ip_route_use_hint deref in fib_validate_source() in an old tree [1]. It appears the bug exists in latest trees. All calls to __in_dev_get_rtnl result. [1] general protection fault, probably for non-canonical address 0xdffffc0000000000: 0000 [#1] SMP KASAN: [0x0000000000000000-0x0000000000000000] CPU: 2 PID: 3257 Comm: syz-executor.3 Not tainted 5.10.0-syzkaller (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2-bpo12+1 04/01/2014 RIP: 0010:fib_validate_source+0xbf/0x1f2 f2 f2 f2 c7 44 20 23 f3 f3 f3 f3 48 89 44 24 78 42 c6 44 20 27 f3 e8 5d 88 48 fc 4c 89 e8 48 c1 e8 03 48 89 44 20 15 98 fc 48 89 5c 24 10 41 bf RSP: 0018:ffff900015fee40 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RDX: 0000000000000000 RSI: 00000000004001eac RDI: fffff880160c64c RBP: fffff800015ff060 R08: 00000000 R10: 0000000000000002 R11: fffff8800f4f90c0 R12: dffffc0000000000 R13: 0000000000000000 R14: 0000000000000000 FS: 00007f938acf6c0(0000) GS:ffff88058c000000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR3: 000000001248e000 CR4: 0000000000352ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR6: 00000000ffff00ff DR7: 0000000000000400 Call Trace: ip_route_use_hint+0x410/0x9b6 [31.085293] +0x2c4/0x1a30 net/ipv4/ip_input.c:327 ip_list_rcv_finish net/ipv4/ip_input.c:612 [inline] ip_sublist_rcv+0x3ed/0x400 [31.085378] +0x422/0x470 net/ipv4/ip_input.c:673 __netif_receive_skb_list_ptype net/core/dev.c:5572 [inline] __netif_receive_skb_list net/core/dev.c:5620 [inline] netif_receive_skb_list net/core/dev.c:5672 [inline] netif_receive_skb_list_internal+0x9f9/0xdc0 net/core/dev.c:5816 xdp_rcv_frames net/bpf/test_run.c:257 [inline] xdp_test_run_batch net/bpf/test_run.c:363 bpf_prog_test_run_xdp+0x81f/0x1170 net/bpf/test_run.c:1376 bpf_prog_test_run syscalls:3736 __sys_bpf+0x45c/0x710 kernel/bpf/syscalls.c:5115 __do_sys_bpf kernel/bpf/syscalls.c:5201 [inline] [31.085453] [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscalls.c:5199
CVE-2024-36898	In the Linux kernel, the following vulnerability has been resolved: gpiolib: cdev: fix uninitialised kfifo If a line is read before being debouncing in software, and the line is subsequently reconfigured to enable edge detection then the allocation of the kfifo. This results in events being written to and read from an uninitialised kfifo. Read events are returned to userspace. If the software debounce is already active.
CVE-2024-36899	In the Linux kernel, the following vulnerability has been resolved: gpiolib: cdev: Fix use after free in lineinfo_changed_notifier_chain as follows: when the GPIO chip device file is being closed by invoking gpio_chrdev_release(), watched_lines is freed. If the lineinfo_changed_nb notifier chain failed due to waiting write rwsem. Additionally, one of the GPIO chip's lines is freed. Consequently, a race condition leads to the use-after-free of watched_lines. Here is the fix: gpio_chrdev_release() --> bitmap_free(cdev->watched_lines) <-- freed --> blocking_notifier_chain_unregister() --> rwsem --> __down_write_common() --> rwsem_down_write_slowpath() --> schedule_preempt_disabled() --> schedule_preempt_disabled() --> gpio_free() --> gpiod_free() --> gpiod_free_commit() --> gpiod_line_state_notify() --> blocking_notifier_call_chain() --> rwsem --> notifier_call_chain() --> lineinfo_changed_notify() --> test_bit(XXXX, cdev->watched_lines) <-- use after free. The issue is that a GPIO line event is being generated for userspace where it shouldn't. However, since the chrdev is being freed, the read that event anyway. To fix the issue, call the bitmap_free() function after the unregistration of lineinfo_changed_notifier_chain.

CVE-2024-36942	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: qca: fix firmware check error path A firmware files before downloading them to the controller but introduced a memory leak in case the sanity checks fail before returning on errors.
CVE-2024-36964	In the Linux kernel, the following vulnerability has been resolved: fs/9p: only translate RWX permissions for plain bits is allowed through, which causes it to be able to set (among others) the suid bit. This was presumably not the intent explicitly and conditionally on .u.
CVE-2024-38577	In the Linux kernel, the following vulnerability has been resolved: rcu-tasks: Fix show_rcu_tasks_trace_gp_kthread() buffer overflow in show_rcu_tasks_trace_gp_kthread() if counters, passed to sprintf() are huge. Counter numbers, if buffer overflow is still possible. Use snprintf() with buffer size instead of sprintf(). Found by Linux Verification Center
CVE-2024-38620	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: HCI: Remove HCI_AMP support Since HCI_AMP controllers no longer has any use so remove it along with the capability of creating AMP controllers. Since we no longer support Primary controllers, as only HCI_PRIMARY is left, this also remove hdev->dev_type altogether.
CVE-2024-38667	In the Linux kernel, the following vulnerability has been resolved: riscv: prevent pt_regs corruption for secondary hart should be reserved for pt_regs. However this is not the case for the idle threads of the secondary boot harts. Their stack may get corrupted. Similar issue has been fixed for the primary hart, see c7cdd96eca28 ("riscv: prevent stack corruption"). However that fix was not propagated to the secondary harts. The problem has been noticed in some CPU hotplug tests where stored several registers on stack, corrupting top of pt_regs structure including status field. As a result, kernel attempts
CVE-2024-39496	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix use-after-free due to race with creation of a block group, we can race with a device replace operation and then trigger a use-after-free on the device (the replace operation). This happens because at btrfs_load_zone_info() we extract a device from the chunk map into the while not under the protection of the device replace rwsem. So if there's a device replace operation happening when the source of the replace operation, we will trigger a use-after-free if before we finish using the device the replace operation enlarging the critical section under the protection of the device replace rwsem so that all uses of the device are done
CVE-2024-39496	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix use-after-free due to race with creation of a block group, we can race with a device replace operation and then trigger a use-after-free on the device (the replace operation). This happens because at btrfs_load_zone_info() we extract a device from the chunk map into the while not under the protection of the device replace rwsem. So if there's a device replace operation happening when the source of the replace operation, we will trigger a use-after-free if before we finish using the device the replace operation enlarging the critical section under the protection of the device replace rwsem so that all uses of the device are done
CVE-2024-39497	In the Linux kernel, the following vulnerability has been resolved: drm/shmem-helper: Fix BUG_ON() on mmap(Fix of check for copy-on-write (COW) mapping in drm_gem_shmem_mmap allows users to call mmap with PROT_WRITE which causes a kernel panic due to BUG_ON in vmf_insert_pfn_prot: BUG_ON((vma->vm_flags & VM_PFNMAP) && is_copy_on_write) == 0) EINVAL early if COW mapping is detected. This bug affects all drm drivers using default shmem helpers. It can be reproduced by: *ptr = mmap(0, size, PROT_WRITE, MAP_PRIVATE, fd, mmap_offset); ptr[0] = 0;
CVE-2024-39507	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix kernel crash problem in concurrent driver need to notify the roce driver to handle this event, but at this time, the roce driver may uninit, then cause kernel status change, need to check whether the roce registered, and when uninit, need to wait link update finish.
CVE-2024-39508	In the Linux kernel, the following vulnerability has been resolved: io_uring/io-wq: Use set_bit() and test_bit() at worker->flags within io_uring/io-wq to address potential data races. The structure io_worker->flags may be accessed concurrently to concurrency issues. When KCSAN is enabled, it reveals data races occurring in io_worker_handle_work and io_worker_activate_free_worker. BUG: KCSAN: data-race in io_worker_handle_work / io_wq_activate_free_worker write to 0xffff8885c4246404 of io_worker_handle_work (io_uring/io-wq.c:434 io_uring/io-wq.c:569) io_wq_worker (io_uring/io-wq.c:?) <snip> read by task 49024 on cpu 5: io_wq_activate_free_worker (io_uring/io-wq.c:?) io_uring/io-wq.c:285) io_wq_enqueue (io_uring/io_uring.c:524) io_req_task_submit (io_uring/io_uring.c:1511) io_handle_tw_list (io_uring/io_uring.c:18daea77cca6 ("Merge tag 'for-linus' of git://git.kernel.org/pub/scm/virt/kvm/kvm"). These races involve writes and reads from different tasks running on different CPUs. To mitigate this, refactor the code to use atomic operations such as set_bit, test_bit, "and" and "or" operations. This ensures thread-safe manipulation of worker flags. Also, move `create_index` to avoid

CVE-2024-39510	<p>In the Linux kernel, the following vulnerability has been resolved: cachefiles: fix slab-use-after-free in cachefiles_ondemand_daemon_read() We got the following issue in a fuzz test of randomly issuing the restore command:</p> <pre>===== BUG: KASAN: slab-use-after-free in cachefiles_ondemand_daemon_read+0xb41/0xb60 Read of size 8 at addr ffff888122e84088 by task ondemand-04-4962 Comm: ondemand-04-dae Not tainted 6.8.0-dirty #564 Call Trace: kasan_report+0x93/0xc0 cachefiles_ondemand_daemon_read+0x169/0xb50 ksys_read+0xf5/0x1e0 Allocated by task 116: kmem_cache_alloc+0x140/0x3a0 cachefiles_lookup_cookie_state_machine+0x43c/0x1230 [...] Freed by task 792: kmem_cache_free+0xfe/0x390 cachefiles_lookup_fscache_cookie_state_machine+0x5c8/0x1230 [...] ===== Following is the process that triggers the issue: mount daemon_thread1 daemon_thread2 ----- cachefiles_withdraw_cookie cachefiles_ondemand_clean_object(object) cachefiles_ondemand_send_req REQ_A = wait_for_completion(&REQ_A->done) cachefiles_daemon_read cachefiles_ondemand_daemon_read REQ_A = cache_msg->object_id = req->object->ondemand->ondemand_id ----- restore ----- cachefiles_ondemand_restore xas_for_each_xas_set_mark(&xas, CACHEFILES_REQ_NEW) cachefiles_daemon_read cachefiles_ondemand_daemon_read REQ_A = copy_to_user(_buffer, msg, n) xa_erase(&cache->reqs, id) complete(&REQ_A->done) ----- close(fd) ----- cachefiles_ondemand_put_object cachefiles_put_object kmem_cache_free(cachefiles_object_jar, object) REQ_A->object->ondemand->ondemand_id = 0 When we see the request within xa_lock, req->object must not have been freed yet, so grab the reference count of object. =====</pre>
CVE-2024-40899	<p>In the Linux kernel, the following vulnerability has been resolved: cachefiles: fix slab-use-after-free in cachefiles_ondemand_daemon_read() We got the following issue in a fuzz test of randomly issuing the restore command:</p> <pre>===== BUG: KASAN: slab-use-after-free in cachefiles_ondemand_daemon_read+0x609/0xab0 Write of size 4 at addr ffff888122e84088 by task ondemand-04-dae/4962 CPU: 11 PID: 4962 Comm: ondemand-04-dae Not tainted 6.8.0-rc7-dirty #542 Call Trace: cachefiles_ondemand_daemon_read+0x609/0xab0 vfs_read+0x169/0xb50 ksys_read+0xf5/0x1e0 Allocated by task 626: kmem_cache_alloc+0x140/0x3a0 cachefiles_lookup_cookie_state_machine+0x43c/0x1230 [...] Freed by task 626: kmem_cache_free+0xfe/0x390 cachefiles_lookup_fscache_cookie_state_machine+0x5c8/0x1230 [...] ===== Following is the process that triggers the issue: mount daemon_thread1 daemon_thread2 ----- cachefiles_ondemand_init object cachefiles_ondemand_daemon_read cachefiles_ondemand_daemon_read REQ_A = kcalloc(sizeof(*req) + data_len) wait_for_completion(&REQ_A->done) cachefiles_daemon_read cachefiles_ondemand_select_req cachefiles_ondemand_get_fd copy_to_user(_buffer, msg, n) process_cache_msg restore ----- cachefiles_ondemand_restore xas_for_each(&xas, req, ULONG_MAX) xas_set_mark(&xas, CACHEFILES_REQ_NEW) cachefiles_daemon_read cachefiles_ondemand_daemon_read REQ_A = cachefiles_ondemand_select_req write(device, req, sizeof(*req)); cachefiles_ondemand_copen xa_erase(&cache->reqs, id) complete(&REQ_A->done) kfree(REQ_A) cachefiles_ondemand_get_unused_fd flags file = anon_inode_getfile(fd_install(fd, file) load = (void *)REQ_A->msg.data; load->fd = fd) issuing a restore command when the daemon is still alive, which results in a request being processed multiple times. To avoid this problem, add an additional reference count to cachefiles_req, which is held while waiting and reading, and then release it. Note that since there is only one reference count for waiting, we need to avoid the same request being completed multiple times. request if it is successfully removed from the xarray. =====</pre>
CVE-2024-40900	<p>In the Linux kernel, the following vulnerability has been resolved: cachefiles: remove requests from xarray during CACHEFILES_DEAD set, we can still read the requests, so in the following concurrency the request may be used after free:</p> <pre>===== cachefiles_ondemand_init object cachefiles_ondemand_daemon_read cachefiles_ondemand_daemon_read REQ_A = kcalloc(sizeof(*req) + data_len) wait_for_completion(&REQ_A->done) cachefiles_daemon_read cachefiles_ondemand_daemon_read dev fd cachefiles_flush_reqs complete(&REQ_A->done) kfree(REQ_A) xa_lock(&cache->reqs); cachefiles_ondemand_read cachefiles_ondemand_read CACHEFILES_OP_READ // req use-after-free !!! xa_unlock(&cache->reqs); xa_destroy(&cache->reqs) Hence request is flushed them to avoid accessing freed requests. =====</pre>
CVE-2024-40910	<p>In the Linux kernel, the following vulnerability has been resolved: ax25: Fix refcount imbalance on inbound connections</p> <p>ax25_release(), we call netdev_put() to decrease the refcount on the associated ax.25 device. However, the execution of ax25_release() never calls netdev_hold(). This imbalance leads to refcount errors, and ultimately to kernel crashes. A typical call trace is as follows:</p> <pre>one of the following errors: refcount_t: decrement hit 0; leaking memory. refcount_t: underflow; use-after-free. [0] ax25_release+0xb2/0x100 ? show_regs+0x64/0x70 ? __warn+0x83/0x120 ? refcount_warn_saturate+0xb2/0x100 ? report_bug+0x1f/0x30 ? handle_bug+0x3e/0x70 ? exc_invalid_op+0x1c/0x70 ? asm_exc_invalid_op+0x1f/0x30 ? refcount_warn_saturate+0xb2/0x100 ax25_release+0x2ad/0x360 __sock_release+0x35/0xa0 sock_close+0x19/0x20 [...] On reboot (or any other event), gets stuck in an infinite loop: unregister_netdevice: waiting for ax0 to become free. Usage count = 0 This patch corrects the refcount imbalance by calling netdev_hold() and ax25_dev_hold() for new connections in ax25_accept(). This makes the logic leading to ax25_accept() correct. In both cases we increment the refcount, which is ultimately decremented in ax25_release().</pre>

CVE-2024-40915	<p>In the Linux kernel, the following vulnerability has been resolved: riscv: rewrite <code>__kernel_map_pages()</code> to fix sleep is a debug function which clears the valid bit in page table entry for deallocated pages to detect illegal memory access. <code>__set_memory()</code> can be called in atomic context, and thus is illegal to sleep. An example warning that this can occur in invalid context at <code>kernel/locking/rwsem.c:1578 in_atomic(): 1, irqs_disabled(): 0, non_block: 0, pid: 2, name: kthre</code> 0 PID: 2 Comm: kthreadd Not tainted 6.9.0-g1d4c6d784ef6 #37 Hardware name: riscv-virtio,qemu (DT) Call Trace: <code>+0x1c/0x24 [<ffffffffff8091ef6e>] show_stack+0x2c/0x38 [<ffffffffff8092baf8>] dump_stack_lvl+0x5a/0x72 [<ffffffffff8003b7ac>] __might_resched+0x104/0x10e [<ffffffffff8003b7f4>] __might_sleep+0x3e/0x62 [<ffffffffff8091ef6e>] __set_memory+0x82/0x2fa [<ffffffffff8000d324>] __kernel_map_pages+0x5a/0xd4 [<ffffffffff8003b7f4>] __vmlinux_node_range+0x196/0x6ba [<ffffffffff80011904>] copy_process+0x72c/0x17ec [<ffffffffff80012f62>] kernel_thread+0x82/0xa0 [<ffffffffff8003552c>] kthreadd+0x14a/0x1be [<ffffffffff809357de>] with <code>apply_to_existing_page_range()</code>. It is fine to not have any locking, because <code>__kernel_map_pages()</code> works with pages are not changed by anyone else in the meantime.</code></p>
CVE-2024-40918	<p>In the Linux kernel, the following vulnerability has been resolved: parisc: Try to fix random segmentation faults in PA8800 and PA8900 processors have had problems with random segmentation faults for many years. Systems with Systems with PA8800 and PA8900 processors have a large L2 cache which needs per page flushing for decent performance. The combined cache in these systems is also more sensitive to non-equivalent aliases than the caches in earlier systems. The faults that I have looked at appear to be memory corruption in memory allocated using <code>mmap</code> and <code>malloc</code>. My first work. On reviewing the cache code, I realized that there were two issues which the existing code didn't handle correctly. The issue is that the present bit in PTEs is racy. 1) PA-RISC caches have a mind of their own and they can speculatively flush the page. This is particularly important on SMP systems. In some of the flush routines, the flush routine would be purged. This was because the flush routine needed the TLB entry to do the flush. 2) My initial approach to try and use <code>flush_cache_page_if_present</code> for all flush operations. This actually made things worse and led to a couple of on me that some lines weren't being flushed because the pte check code was racy. This resulted in random inequivalency. <code>__flush_cache_page</code> <code>tmpalias</code> flush sets up its own TLB entry and it doesn't need the existing TLB entry. As long as we can get the pfn and physical address of the page. We can also purge the TLB entry for the page before doing the special TLB entry that inhibits cache move-in. When switching page mappings, we need to ensure that lines are reflushed. This includes flushes for user and kernel pages. After modifying the code to use <code>tmpalias</code> flushes, it became clear that the problem was fully resolved. The frequency of faults was worse on systems with a 64 MB L2 (PA8900) and systems with more cache. To flush <code>cache_page_if_present</code> to detect pages that couldn't be flushed triggered frequently on some systems. Helge flushed and found that the PTE was either cleared or for a swap page. Ignoring pages that were swapped out seemed problematic. I looked at routines related to <code>pte_clear</code> and noticed <code>ptep_clear_flush</code>. The default implementation just flushes the page. It is obvious that on parisc we need to flush the cache page as well. If we don't flush the cache page, stale lines will be left. Once a PTE is cleared, there is no way to find the physical address associated with the PTE and flush the associated page. The updated change with a parisc specific version of <code>ptep_clear_flush</code>. It fixed the random data corruption on Helge's system. At this point, I realized that I could restore the code where we only flush in <code>flush_cache_page_if_present</code> if the page has been accessed. We need to flush the cache when the accessed bit is cleared in <code>---truncated---</code></p>
CVE-2024-40927	<p>In the Linux kernel, the following vulnerability has been resolved: xhci: Handle TD clearing for multiple streams correctly. Multiple TDs might be in flight when an endpoint is stopped. We need to issue a Set TR Dequeue Pointer for each, and the caches cleared. Change the logic so that any N>1 TDs found active for different streams are deferred until the first TD is cleared. <code>xhci_invalidate_cancelled_tds()</code> again from <code>xhci_handle_cmd_set_deq()</code> to queue another command until we are done. "error"/"should never happen" paths to ensure we at least clear any affected TDs, even if we can't issue a command to the device loudly with an <code>xhci_warn()</code> if this ever happens. This problem case dates back to commit e9df17eb1408 ("USB: xhci: add rings per endpoint.") early on in the XHCI driver's life, when stream support was first added. It was then identified in commit 674f8438c121 ("xhci: split handling halted endpoints into two steps"), which added a FIXME comment about changing the behavior as far as I can tell, though the new logic made the problem more obvious). Then later, in commit 94f339147fc3 ("xhci: Fix URBs."), it was acknowledged again. [Mathias: commit 94f339147fc3 ("xhci: Fix URBs.") was a targeted regression fix to the previously mentioned patch. Users reported issues with usb stuck after this rolled back the TD clearing of multiple streams to its original state.] Apparently the commit author was aware of the problem. It was still mentioned as a FIXME, an <code>xhci_dbg()</code> was added to log the problem condition, and the remaining issue was not fixed. The choice of making the log type <code>xhci_dbg()</code> for what is, at this point, a completely unhandled and known broken condition, it guarantees that no actual users would see the log in production, thereby making it nigh undebuggable (indeed, even if it does, it doesn't really hint at there being a problem at all). It took me *months* of random xHC crashes to finally find a reliable debug session, which could all have been avoided had this unhandled, broken condition been actually reported with a patch. It was intentionally left in unfixed (never mind that it shouldn't have been left in at all). > Another fix to solve clearing the TDs is needed, but not as urgent. 3 years after that statement and 14 years after the original bug was introduced, I think it is time next time let's not leave bugs unfixed (that are actually worse than the original bug), and let's actually get people to report crashes and IOMMU faults with UAS devices when handling errors/faults. Easiest repro is to use 'hdparm' to mark a device as bad, then 'cat /dev/sdX > /dev/null' in a loop. At least in the case of JMicron controllers, the read errors end up having requests to different streams and the one that didn't get cleared properly ends up faulting the xHC entirely when it tries to access the been unmapped, referred to by the stale TDs. This normally happens quickly (after two or three loops). After this fix, I experienced no xHC failures, with all read errors recovered properly. Repro'd and tested on an Apple M1 Mac with IOMMU, this bug would instead silently corrupt freed memory, making this a <code>---truncated---</code></p>

CVE-2024-40947	<p>In the Linux kernel, the following vulnerability has been resolved: ima: Avoid blocking in RCU read-side critical section. BUG: unable to handle kernel NULL pointer dereference at 0000000000000010 PGD 42f873067 P4D 0 Oops: 0000000000000000 1286325 Comm: kubeletmonit.sh Kdump: loaded Tainted: P Hardware name: QEMU Standard PC (i440FX + PIIX, 0010:ima_match_policy+0x84/0x450 Code: 49 89 fc 41 89 cf 31 ed 89 44 24 14 eb 1c 44 39 7b 18 74 26 41 83 ff 00 9c 01 00 00 <44> 85 73 10 74 ea 44 8b 6b 14 41 f6 c5 01 75 d4 41 f6 c5 02 74 0f RSP: 0018:ff1570009e07a80 EIP: 0018:ff1570009e07a80 RBX: 0000000000000000 RCX: 0000000000000200 RDX: ffffffffad8dc7c0 RSI: 0000000024924925 RDI: ff3e2718 R08: 0000000000000000 R09: ffffffffabfce739 R10: ff3e27810cc42400 R11: 0000000000000000 R12: ff3e27818 R13: 0000000000000000 R15: 0000000000000001 FS: 00007f5195b51740(0000) GS:ff3e278b12d40000(0000) knlGS: 0000000000000000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000010 CR3: 0000000626d24002 CR4: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000000 +0x22/0x30 process_measurement+0xb0/0x830 ? page_add_file_rmap+0x15/0x170 ? alloc_set_pte+0x269/0x4c0 ? simple_xattr_get+0x75/0xa0 ? selinux_file_open+0x9d/0xf0 ima_file_check+0x64/0x90 path_openat+0x571/0x17 page_counter_try_charge+0x57/0xc0 ? files_cgroup_alloc_fd+0x38/0x60 ? __alloc_fd+0xd4/0x250 ? do_sys_open+0x1bd/0x250 do_syscall_64+0x5d/0x1d0 entry_SYSCALL_64_after_hwframe+0x65/0xca Commit c7423dbdbc9c9c introduced call to ima_lsm_copy_rule within a RCU read-side critical section which could potentially sleep, which implies a possible sleep and violates limitations of RCU read-side critical sections on non-PREEMPT systems. Sleep in ima_lsm_copy_rule might cause synchronize_rcu() returning early and break RCU protection, allowing a UAF to happen. The root cause follows: Thread A Thread B ima_match_policy rcu_read_lock ima_lsm_update_rule synchronize_rcu ==> synchronize_rcu returns early kfree(entry) entry = entry->next ==> UAF happens and entry now becomes dangling ==> Accessing entry might cause panic. To fix this issue, we are converting all kmallocc that is called with GFP_ATOMIC. [PM: fixed missing comment, long lines, !CONFIG_IMA_LSM_RULES case]</p>
CVE-2024-40953	<p>In the Linux kernel, the following vulnerability has been resolved: KVM: Fix a data race on last_boosted_vcpu in kvm_vcpu_ioctl_run. {READ,WRITE}_ONCE() to access kvm->last_boosted_vcpu to ensure the loads and stores are atomic. In the extreme case, if it tears the stores, it's theoretically possible for KVM to attempt to get a vCPU using an out-of-bounds index, e.g. if the index is 0x01 and is paired with a 32-bit load on a VM with 257 vCPUs: CPU0 CPU1 last_boosted_vcpu = 0xff; (last_boosted_vcpu = 0x01; i = (last_boosted_vcpu = 0x1ff) last_boosted_vcpu[7:0] = 0x00; vcpu = kvm->vcpu_array[0x1ff]; As detected in kvm_vcpu_on_spin [kvm] / kvm_vcpu_on_spin [kvm] write to 0xffff90025a92344 of 4 bytes by task 4340 on cpu 0: kvm_vcpu_ioctl_run (arch/x86/kvm/vmx/vmx.c:5929) kvm_intel vmx_handle_exit (arch/x86/kvm/vmx/vmx.c:6606) kvm_intel vcpu_run (arch/x86/kvm/x86.c:11107 arch/x86/kvm/x86.c:11211) kvm_vcpu_ioctl_run (arch/x86/kvm/x86.c:?) kvm_vcpu_ioctl (arch/x86/kvm/vmx/vmx.c:?) kvm __se_sys_ioctl (fs/ioctl.c:52 fs/ioctl.c:890) x64_sys_ioctl (arch/x86/entry/syscall_64.c:33) do_syscall_64 (arch/x86/entry/common.c:?) entry_SYSCALL_64.S:130) read to 0xffff90025a92344 of 4 bytes by task 4342 on cpu 4: kvm_vcpu_on_spin (arch/x86/kvm/vmx/vmx.c:5929) kvm_intel vmx_handle_exit (arch/x86/kvm/vmx/vmx.c:?) arch/x86/kvm/vmx/vmx.c:11107 arch/x86/kvm/x86.c:11211) kvm_vcpu_ioctl_run (arch/x86/kvm/vmx/vmx.c:?) kvm_vcpu_ioctl (arch/x86/kvm/vmx/vmx.c:?) kvm __se_sys_ioctl (fs/ioctl.c:52 fs/ioctl.c:904 fs/ioctl.c:890) __x64_sys_ioctl (arch/x86/entry/syscall_64.c:33) do_syscall_64 (arch/x86/entry/common.c:?) entry_SYSCALL_64_after_hwframe (arch/x86/entry/common.c:?) -> 0x00000000</p>
CVE-2024-40965	<p>In the Linux kernel, the following vulnerability has been resolved: i2c: lpi2c: Avoid calling clk_get_rate during transfer. clk_get_rate for each transfer, lock the clock rate and cache the value. A deadlock has been observed while adding a new clock provider. When this clock provider adds its clock, the clk mutex is locked already, it needs to access i2c, which in return needs the clk mutex.</p>
CVE-2024-40967	<p>In the Linux kernel, the following vulnerability has been resolved: serial: imx: Introduce timeout when waiting on USR2_TXDC to be set, we avoid a potential deadlock. In case of the timeout, there is not much we can do but wait and optimistically try to continue.</p>
CVE-2024-40969	<p>In the Linux kernel, the following vulnerability has been resolved: f2fs: don't set RO when shutting down f2fs. Shutting down f2fs due to readonly, which causes a deadlock like below. f2fs_ioc_shutdown(F2FS_GOING_DOWN_FULLSYNC) is called. f2fs_freeze_super - f2fs_stop_checkpoint() - f2fs_handle_critical_error - sb_start_write - set RO - waiting - bdev_thaw - sb_rdonly() - f2fs_stop_discard_thread -> wait for kthread_stop(discard_thread);</p>
CVE-2024-40970	<p>In the Linux kernel, the following vulnerability has been resolved: Avoid hw_desc array overrun in dw-axi-dmac. In dw-axi-dmac, each descriptor is composed by 3 segments, resulting in the DMA channel descriptors allocated to be 9. Since the descriptors are allocated, this scenario would result in a kernel panic (hw_desc array will be overrun). To fix this, we need to update the axi_dma_desc structure, where we keep the number of allocated hw_descs (axi_desc_alloc()) and use it in axi_dma_desc correctly. Additionally I propose to remove the axi_chan_start_first_queued() call after completing the transfer, since descriptors can be interrupted and transfer ignored due to DMA channel not being enabled).</p>
CVE-2024-40971	<p>In the Linux kernel, the following vulnerability has been resolved: f2fs: remove clear SB_INLINECRYPT flag in clear and re-set. If create new file or open file during this gap, these files will not be encrypted. This could lead to data corruption if wrappedkey_v0 is enable. Thread A: -f2fs_remount -f2fs_file_open or f2fs_new_file -> set SB_INLINECRYPT flag -fscrypt_select_encryption_impl -parse_options <- set SB_INLINECRYPT again</p>
CVE-2024-40973	<p>In the Linux kernel, the following vulnerability has been resolved: media: mtk-vcdec: potential null pointer dereference. devm_kzalloc() needs to be checked to avoid NULL pointer dereference. This is similar to CVE-2022-3113.</p>

[illegible]

96

CVE-2024-41035	In the Linux kernel, the following vulnerability has been resolved: USB: core: Fix duplicate endpoint bug by clearing identified a bug in usbcore (see the Closes: tag below) caused by our assumption that the reserved bits in an endpoint always be 0. As a result of the bug, the endpoint_is_duplicate() routine in config.c (and possibly other routines as well) for distinct endpoints, even though they have the same direction and endpoint number. This can lead to confusion, descriptors with matching endpoint numbers and directions, where one was interrupt and the other was bulk). To fix bEndpointAddress when we parse the descriptor. (Note that both the USB-2.0 and USB-3.1 specs say these bits are to make a copy of the descriptor earlier in usb_parse_endpoint() and use the copy instead of the original when checking
CVE-2024-41036	In the Linux kernel, the following vulnerability has been resolved: net: ks8851: Fix deadlock with the SPI chip variants are actually functional then there is a deadlock with the 'statelock' spinlock between ks8851_start_xmit_spi and ks8851_lockup - CPU#0 stuck for 27s! call trace: queued_spin_lock_slowpath+0x100/0x284 do_raw_spin_lock+0x34/0x44 ks8851_start_xmit+0x14/0x20 netdev_start_xmit+0x40/0x6c dev_hard_start_xmit+0x6c/0xbc sch_direct_xmit+0x10/0x10 qdisc_run+0x24/0x3c net_tx_action+0xf8/0x130 handle_softirqs+0x1ac/0x1f0 __do_softirq+0x14/0x20 ____do_softirq+0x3c/0x58 do_softirq_own_stack+0x1c/0x28 __irq_exit_rcu+0x54/0x9c irq_exit_rcu+0x10/0x1c e11_interrupt+0x10/0x1c e11h_64_irq+0x64/0x68 __netif_schedule+0x6c/0x80 netif_tx_wake_queue+0x38/0x48 ks8851_irq+0xb8/0x2c8 irq_thread+0x10c/0x1b0 kthread+0xc8/0xd8 ret_from_fork+0x10/0x20 This issue has not been identified earlier because test cases and so spinlocks were actually NOPs. Now use spin_(un)lock_bh for TX queue related locking to avoid execution to a deadlock.
CVE-2024-41040	In the Linux kernel, the following vulnerability has been resolved: net/sched: Fix UAF when resolving a clash KASAN: BUG: KASAN: slab-use-after-free in tcf_ct_flow_table_process_conn+0x12b/0x380 [act_ct] Read of size 1 at address 0xffffc90000000000 handler130/6469 Call Trace: <IRQ> dump_stack_lvl+0x48/0x70 print_address_description.constprop.0+0x33/0x33 +0xd0/0x120 __asan_load1+0x6c/0x80 tcf_ct_flow_table_process_conn+0x12b/0x380 [act_ct] tcf_ct_act+0x88/0x100 +0xf8/0x1f0 fl_classify+0x355/0x360 [cls_flower] __tcf_classify+0x1fd/0x330 tcf_classify+0x21c/0x3c0 sch_handle_ingress.constprop.0+0xb25/0x1510 __netif_receive_skb_core.constprop.0+0x220/0x4c0 netif_receive_skb_list_core+0x220/0x4c0 netif_receive_skb_list_internal+0x446/0x620 napi_complete_done+0x157/0x3d0 gro_cell_poll+0xcf/0x100 __napi_poll+0x65/0x310 net_rx_action+0x30c/0x5c0 +0x82/0xc0 irq_exit_rcu+0xe/0x20 common_interrupt+0xa1/0xb0 </IRQ> <TASK> asm_common_interrupt+0x2/0x2 kasan_save_stack+0x38/0x70 kasan_set_track+0x25/0x40 kasan_save_alloc_info+0x1e/0x40 __kasan_krealloc+0x10/0x10 nf_ct_ext_add+0xed/0x230 [nf_conntrack] tcf_ct_act+0x1095/0x1350 [act_ct] tcf_action_exec+0xf8/0x1f0 fl_classify+0x355/0x360 [cls_flower] __tcf_classify+0x1fd/0x330 tcf_classify+0x21c/0x3c0 sch_handle_ingress.constprop.0+0x220/0x4c0 netif_receive_skb_list_core+0x220/0x4c0 netif_receive_skb_list_internal+0x446/0x620 napi_complete_done+0x157/0x3d0 gro_cell_poll+0xcf/0x100 __napi_poll+0x65/0x310 net_rx_action+0x30c/0x5c0 __do_softirq+0x14f/0x491 Freed by task 6469: kasan_save_free_info+0x25/0x40 kasan_save_free_info+0x2b/0x60 __kasan_slab_free+0x180/0x1f0 __kasan_slab_free+0x12/0x30 s_kmem_cache_free+0x1a2/0x2f0 kfree+0x78/0x120 nf_conntrack_free+0x74/0x130 [nf_conntrack] nf_ct_destroy nf_ct_resolve_clash+0x529/0x5d0 [nf_conntrack] nf_ct_resolve_clash+0xf6/0x490 [nf_conntrack] __nf_conntrack tcf_ct_act+0x12ad/0x1350 [act_ct] tcf_action_exec+0xf8/0x1f0 fl_classify+0x355/0x360 [cls_flower] __tcf_classify sch_handle_ingress.constprop.0+0x220/0x4c0 netif_receive_skb_core.constprop.0+0xb25/0x1510 __netif_receive_skb_list_internal+0x446/0x620 napi_complete_done+0x157/0x3d0 gro_cell_poll+0xcf/0x100 __napi_poll+0x65/0x310 net_rx_action+0x30c/0x5c0 __do_softirq+0x14f/0x491 The ct may be dropped if a clash has been resolved but is still passed to for further usage. This issue can be fixed by retrieving ct from skb again after confirming conntrack.
CVE-2024-41041	In the Linux kernel, the following vulnerability has been resolved: udp: Set SOCK_RCU_FREE earlier in udp_lib_lookup() in udp_v4_early_demux(). In udp_v[46]_early_demux() and sk_lookup(), we do not touch the refcount of the lock and sk_lookup(), so there could be a small race window: CPU1 CPU2 ---- udp_v4_early_demux() udp_lib_get_sock() __udp4_lib_demux_lookup() - DEBUG_NET_WARN_ON_ONCE(sk_is_refcounted(sk)); - sock_set_flag(sk, SOCK_RCU_FREE); bug in TCP and fixed it in commit 871019b22d1b ("net: set SOCK_RCU_FREE before inserting socket into hashtable") [0]: WARNING: CPU: 0 PID: 11198 at net/ipv4/udp.c:2599 udp_v4_early_demux+0x481/0xb70 net/ipv4/udp.c:2599 11198 Comm: syz-executor.1 Not tainted 6.9.0-g93bda33046e7 #13 Hardware name: QEMU Standard PC (i440FX) gd239552ce722-prebuilt.qemu.org 04/01/2014 RIP: 0010:udp_v4_early_demux+0x481/0xb70 net/ipv4/udp.c:2599 e9 31 ff d3 e3 81 e3 bf ef ff ff 89 de e8 2c 74 15 fe 85 db 0f 85 02 06 00 00 e8 9f 7a 15 fe <0f> 0b e8 98 7a 15 fe 4 52 RSP: 0018:ffffc90000ce3fa58 EFLAGS: 00010293 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000000000 RSI: ffffffff8318c2f1 RDI: 0000000000000001 RBP: fffff88805a2dd6e0 R08: 0000000000000001 R09: 0000000000000000 R11: 0001ffffffffff R12: fffff88805a2dd680 R13: 0000000000000007 R14: fffff88800923f900 R15: fffff888054560 GS:ffff88807dc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR4: 0000000000000000 CR8: 0000000000000000 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR4: 0000000000000000 DR5: 0000000000000000 DR6: 0000000000000000 DR7: 0000000000000000 PKRU: 55555554 Call Trace: <TASK> ip_rcv_finish_core.constprop.0+0x16c/0x180 net/ipv4/ip_input.c:569 __netif_receive_skb_one_core+0xb3/0xe0 net/core/dev.c:5624 __netif_receive_skb_list_internal net/core/dev.c:5824 [inline] netif_receive_skb_core.constprop.0+0xb25/0x1510 net/core/dev.c:5884 tun_get_user+0x24db/0x2c50 drivers/net/tun.c:2002 tun_chr_write_iter+0x107/0x1a0 drivers/net/tun.c:2048 new_vfs_write+0x76f/0x8d0 fs/read_write.c:590 ksys_write+0xbf/0x190 fs/read_write.c:643 __do_sys_write fs/read_write.c:652 [inline] __x64_sys_write+0x41/0x50 fs/read_write.c:652 x64_sys_call+0xe66/0x1990 arch/x86/entry/common.c:83 RIP: 0033:0x7fc44a68bc1f Code: 89 54 24 18 48 89 74 24 10 89 7c 24 08 e8 e9 cf f5 ff 48 8b 54 24 18 48 8b 74 24 05 <48> 3d 00 f0 ff ff 77 31 44 89 c7 48 89 44 24 08 e8 3c d0 f5 ff 48 RSP: 002b:00007fc449126c90 EFLAGS: 00000000 RAX: ffffffff8318c2f1 RBX: 0000000000000004 RCX: 00007fc44a68bc1f R ---truncated---

CVE-2024-41042	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: prefer nft_chain_validate nft detection because a cycle will result in a call stack overflow (ctx->level >= NFT_JUMP_STACK_SIZE). It also fixes nft_lookup, so there appears no reason to iterate the maps again. nf_tables_check_loops() and all its helper functions save time significantly, from 23s down to 12s. This also fixes a crash bug. Old loop detection code can result in unbounded loops was hit at Oops: stack guard page: 0000 [#1] PREEMPT SMP KASAN CPU: 4 PID: 1539 Comm: nft Not tainted 6.8.0 during validation of register stores. I can't see any actual reason to attempt to check for this from nft_validate_registers in progress, so we don't have a full picture of the rule graph. For nf-next it might make sense to either remove it or refactor case we could catch an error earlier (for improved error reporting to userspace).
CVE-2024-41044	In the Linux kernel, the following vulnerability has been resolved: ppp: reject claimed-as-LCP but actually malformed packets assumes valid LCP packets (with code from 1 to 7 inclusive), add 'ppp_check_packet()' to ensure that LCP packet length is bytes, and reject claimed-as-LCP but actually malformed data otherwise.
CVE-2024-41046	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: lantiq_etop: fix double free in detach descriptor is never incremented which results in the same skb being released multiple times.
CVE-2024-41048	In the Linux kernel, the following vulnerability has been resolved: skmsg: Skip zero length skb in sk_msg_recvmsg() (t_sockmap_basic) on a Loongarch platform, the following kernel panic occurs: [...] Oops[#1]: CPU: 22 PID: 2824 C0000000 #18 Hardware name: LOONGSON Dabieshan/Loongson-TC542F0, BIOS Loongson-UDK2018 ... ra: 9000000000000000 ERA: 90000000004162774 copy_page_to_iter+0x74/0x1c0 CRMD: 000000b0 (PLV0 -IE -DA +PG DACF=CC DA ... (PPLV0 +PIE +PWE) EUEN: 00000007 (+FPE +SXE +ASXE -BTE) ECFG: 00071c1d (LIE=0,2-4,10-12 VS=7) ... ESubCode=0) BADV: 0000000000000040 PRID: 0014c011 (Loongson-64bit, Loongson-3C5000) Modules linked in: xt_MASQUERADE xt_conntrack Process test_progs (pid: 2824, threadinfo=0000000000863a31, task=...) Stack : copy_page_to_iter+0x74/0x1c0 [<900000000048bf6c0>] sk_msg_recvmsg+0x120/0x560 [<900000000049f2b90>] tcp_v4_rcv [<900000000049aae34>] inet_recvmsg+0x54/0x100 [<9000000000481ad5c>] sock_recvmsg+0x7c/0xe0 [<9000000000481e27c>] sys_recvfrom+0x1c/0x40 [<90000000004c076ec>] do_syscall+0x8c/0xc0 [<900000000037f---[end trace 0000000000000000]--- Kernel panic - not syncing: Fatal exception Kernel relocated by 0x3510000 . 0x90000000004d70000 .bss @ 0x90000000006469400 ---[end Kernel panic - not syncing: Fatal exception]--- [...] T sockmap_skb_verdict_shutdown subtest in sockmap_basic. This crash is because a NULL pointer is passed to page_address() to the different implementations depending on the architecture, page_address(NULL) will trigger a panic on Loongson. This bug was hidden on x86 platform for a while, but now it is exposed on Loongarch platform. The root cause is that we put on the queue. This zero length skb is a TCP FIN packet, which was sent by shutdown(), invoked in test_sockmap_SHUT_WR); In this case, in sk_psock_skb_ingress_enqueue(), num_sge is zero, and no page is put to this sge (see test_sockmap_empty_sge is queued into ingress_msg list. And in sk_msg_recvmsg(), this empty sge is used, and a NULL page is passed to copy_page_to_iter(), which passes it to kmap_local_page() and to page_address(), then kernel panics. To solve this issue, So in sk_msg_recvmsg(), if copy is zero, that means it's a zero length skb, skip invoking copy_page_to_iter(). We added a check copy_page_to_iter to check for is_fin in tcp_bpf.c.
CVE-2024-41049	In the Linux kernel, the following vulnerability has been resolved: filelock: fix potential use-after-free in posix_lock_file_wait warning in trace_posix_lock_inode(). The request pointer had been changed earlier to point to a lock entry that was freed. The tracepoint could fire, another task raced in and freed that lock. Fix this by moving the tracepoint inside the spinlock happen.
CVE-2024-41055	In the Linux kernel, the following vulnerability has been resolved: mm: prevent dereferencing NULL ptr in pf_n_section_sparssemem: fix race in accessing memory_section->usage") changed pf_n_section_valid() to add a READ_ONCE() before section_deactivate() where ms->usage can be cleared. The READ_ONCE() call, by itself, is not enough to prevent clearing its value before dereferencing it.
CVE-2024-41059	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix uninitialized-value in copy_name [syzbot report] value in sized_strncpy+0xc4/0x160 sized_strncpy+0xc4/0x160 copy_name+0x2af/0x320 fs/hfsplus/xattr.c:411 hfsplus_xattr+0x1f3/0x6b0 fs/hfsplus/xattr.c:840 path_listxattr fs/xattr.c:876 [online] __se_sys_listxattr fs/xattr.c:873 [online] __x64_sys_listxattr+0x16b/0x2f0 fs/xattr.c:873 x64_sys_call+0x2ba/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:195 do_syscall_x64 arch/x86/entry/common.c:52 [online] do_syscall_64+0xc0/0x100 include/linux/SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3877 [inline] kmalloc_trace+0x57b/0xbe0 mm/slub.c:4065 kmalloc include/linux/slab.h:628 [inline] hfsplus_listxattr+0x4cc/0x100 fs/xattr.c:493 [online] listxattr+0x1f3/0x6b0 fs/xattr.c:840 path_listxattr fs/xattr.c:864 [online] __do_sys_listxattr fs/xattr.c:873 [online] __x64_sys_listxattr+0x16b/0x2f0 fs/xattr.c:873 x64_sys_call+0x2ba/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:195 do_syscall_x64 arch/x86/entry/common.c:52 [online] do_syscall_64+0xc0/0x100 [Fix] When allocating memory to strbuf, initialize memory to 0.
CVE-2024-41060	In the Linux kernel, the following vulnerability has been resolved: drm/radeon: check bo_va->bo is non-NULL before radeon_vm_clear_freed might clear bo_va->bo, so we have to check it before dereferencing it.
CVE-2024-41061	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix array-index-out-of-bound access in dml2_calculate_rq_and_dlg_params() because the value of out_lowest_state_idx array can be greater than 1. [How] Currently dml2 core specifies identical values for all FCLKChangeSupport elements to avoid out of bounds access.

CVE-2024-41062	In the Linux kernel, the following vulnerability has been resolved: bluetooth/l2cap: sync sock recv cb and release T call to close the sock and hci_rx_work, where the former releases the sock and the latter accesses it without lock pr hci_rx_work l2cap_sock_release hci_acldata_packet l2cap_sock_kill l2cap_recv_frame sk_free l2cap_conless_cha processes the data that needs to be received before the sock is closed, then everything is normal; Otherwise, the wo receiving data. Add a chan mutex in the rx callback of the sock to achieve synchronization between the sock releas to NULL, avoid others use invalid sock pointer.
CVE-2024-41063	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_core: cancel all works upon hci_ calling hci_release_dev() from hci_error_reset() due to hci_dev_put() from hci_error_reset() can cause deadlock at is called from hdev->req_workqueue which destroy_workqueue() needs to flush. We need to make sure that hdev-> are queued into hdev->workqueue and hdev->{power_on,error_reset} which are queued into hdev->req_workqueue destroy_workqueue(hdev->workqueue); destroy_workqueue(hdev->req_workqueue); are called from hci_release_ items from hci_unregister_dev() as soon as hdev->list is removed from hci_dev_list.
CVE-2024-41064	In the Linux kernel, the following vulnerability has been resolved: powerpc/eeh: avoid possible crash when edev-> during eeh_pe_report_edev(), edev->pdev will change and can cause a crash, hold the PCI rescan/remove lock whi
CVE-2024-41065	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Whitelist dtl slub object for co trace log from /sys/kernel/debug/powerpc/dtl/cpu-* results in a BUG() when the config CONFIG_HARDENED_U kernel BUG at mm/usercopy.c:102! Oops: Exception in kernel mode, sig: 5 [#1] LE PAGE_SIZE=64K MMU=Rad Modules linked in: xfs libcrc32c dm_service_time sd_mod t10_pi sg ibmvfc scsi_transport_fc ibmveth pseries_wd dm_log dm_mod fuse CPU: 27 PID: 1815 Comm: python3 Not tainted 6.10.0-rc3 #85 Hardware name: IBM,9040- of:IBM,FW1060.00 (NM1060_042) hv:phyp pSeries NIP: c0000000005d23d4 LR: c0000000005d23d0 CTR: 0000 TRAP: 0700 Not tainted (6.10.0-rc3) MSR: 800000000029033 <SF,EE,ME,IR,DR,RI,LE> CR: 2828220f XER: 0 IRQMASK: 0 [... GPRs omitted ...] NIP [c0000000005d23d4] usercopy_abort+0x78/0xb0 LR [c0000000005d23d0] usercopy_abort+0x74/0xb0 (unreliable) __check_heap_object+0xf8/0x120 check_heap_object+0x218/0x240 __ch +0x17c/0x2c4 full_proxy_read+0x8c/0x110 vfs_read+0xdc/0x3a0 ksys_read+0x84/0x144 system_call_exception+ +0x15c/0x2ec --- interrupt: 3000 at 0x7fff81f3ab34 Commit 6d07d1cd300f ("usercopy: Restrict non-usercopy cach whitelisted areas in slab/slub objects can be copied to userspace when usercopy hardening is enabled using CONF contains hypervisor dispatch events which are expected to be read by privileged users. Hence mark this safe for use usersize=DISPATCH_LOG_BYTES to whitelist the entire object.
CVE-2024-41066	In the Linux kernel, the following vulnerability has been resolved: ibmvnic: Add tx check to prevent skb leak Below a reference to an skb during transmit: tx_buff[free_map[consumer_index]]->skb = new_skb; free_map[consumer_ consumer_index ++; Where variable data looks like this: free_map == [4, IBMVNIC_INVALID_MAP, IBMVNIC tx_buff == [skb=null, skb=<ptr>, skb=<ptr>, skb=null, skb=null] The driver has checks to ensure that free_map[co there was no check to ensure that this index pointed to an unused/null skb address. So, if, by some chance, our free then we were previously risking an skb memory leak. This could then cause tcp congestion control to stop sending Therefore, add a conditional to ensure that the skb address is null. If not then warn the user (because this is still a b pointer to prevent memleak/tcp problems.
CVE-2024-41067	In the Linux kernel, the following vulnerability has been resolved: btrfs: scrub: handle RST lookup error correctly RST feature, it would crash the following ASSERT() inside scrub_read_endio(): ASSERT(sectors->nr < stripe->nr_s dump from btrfs_get_raid_extent_offset(), as we failed to find the RST entry for the range. [CAUSE] Inside scrub allocated a new bbio we immediately called btrfs_map_block() to make sure there was some RST range covering th we immediately call endio for the bbio, while the bbio is newly allocated, it's completely empty. Then inside scrub find the sector number (as bi_sector is no longer reliable if the bio is submitted to lower layers). And since the bio i any sector matching the sector, and return sectors->nr == stripe->nr_sectors, triggering the ASSERT(). [FIX] Instead a new bbio, call btrfs_map_block() first. Since our only objective of calling btrfs_map_block() is only to update str btrfs_alloc_bio(). This new timing would avoid the problem of handling empty bbio completely, and in fact fixes a if the submission thread is the only owner of the pending_io, the scrub would never finish (since we didn't decrease cause of RST lookup failure still needs to be addressed.
CVE-2024-41068	In the Linux kernel, the following vulnerability has been resolved: s390/scslp: Fix scslp_init() cleanup on failure If s up: if there are multiple failing calls to scslp_init() scslp_state_change_event will be added several times to scslp_reg warning: -----[cut here]----- list_add double add: new=000003ffe1598c10, prev=000003ffe1598bf0, no CPU: 0 PID: 1 at lib/list_debug.c:35 __list_add_valid_or_report+0xde/0xf8 CPU: 0 PID: 1 Comm: swapper/0 Not 0404c00180000000 000003ffe0d6076a (__list_add_valid_or_report+0xe2/0xf8) R:0 T:1 IO:0 EX:0 Key:0 M:1 W: Trace: [<000003ffe0d6076a>] __list_add_valid_or_report+0xe2/0xf8 [<000003ffe0d60766>] __list_add_valid_or scslp_init+0x40e/0x450 [<000003ffe0009f2>] do_one_initcall+0x42/0x1e0 [<000003ffe15b77a6>] do_initcalls+0 kernel_init_freeable+0x1ba/0x1f8 [<000003ffe0d6650e>] kernel_init+0x2e/0x180 [<000003ffe000301c>] __ret_f ret_from_fork+0xa/0x30 Fix this by removing scslp_state_change_event from scslp_reg_list when scslp_init() fails.
CVE-2024-41069	In the Linux kernel, the following vulnerability has been resolved: ASoC: topology: Fix references to freed memor release memory used by it, so having pointer references directly into topology file contents is wrong. Use devm_kn

CVE-2024-41070	In the Linux kernel, the following vulnerability has been resolved: KVM: PPC: Book3S HV: Prevent UAF in kvm. AI reported a possible use-after-free (UAF) in kvm_saprr_tce_attach_iommu_group(). It looks up `stt` from tablefd doing fdput() on the returned fd. After the fdput() the tablefd is free to be closed by another thread. The close calls release_saprr_tce_table() (via call_rcu()) which frees `stt`. Although there are calls to rcu_read_lock() in kvm_saprr not sufficient to prevent the UAF, because `stt` is used outside the locked regions. With an artificial delay after the triggers the race, KASAN detects the UAF: BUG: KASAN: slab-use-after-free in kvm_saprr_tce_attach_iommu_group+0xc000200027552c30 by task kvm-vfio/2505 CPU: 54 PID: 2505 Comm: kvm-vfio Not tainted 6.10.0-rc3-next-20240611-g1851b2a06 PowerNV Call Trace: dump_stack_lvl+0xb4/0x108 kasan_report+0x118/0x2b0 __asan_load4+0xb8/0xd0 kvm_saprr_tce_attach_iommu_group+0x298/0x720 [kvm] kvm_device_ioctl+0x144/0x240 [kvm] sys_ioctl+0x62c/0x1810 system_call_exception+0x190/0x440 system_call+0x10/0x10 by task 0: ... kfree+0xec/0x3e0 release_saprr_tce_table+0xd4/0x11c [kvm] rcu_core+0x568/0x16a0 handle_softirq+0x6c/0x90 do_softirq_own_stack+0x58/0x90 __irq_exit_rcu+0x218/0x2d0 irq_exit+0x30/0x80 arch_local_irq_return_i801+0x1c/0x30 cpuidle_enter_state+0x134/0x5cc cpuidle_enter+0x6c/0xb0 call_cpuidle+0x7c/0x100 do_idle+0x394/0x398 start_secondary+0x3fc/0x410 start_secondary_prolog+0x10/0x14 Fix it by delaying the fdput() until `stt` is no longer in use. To keep the patch minimal add a call to fdput() at each of the existing return paths. Future work can consider a cleanup. With the fix in place the test case no longer triggers the UAF.
CVE-2024-41071	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: Avoid address calculations via >n_channels must be set before req->channels[] can be used. This patch fixes one of the issues encountered in [1]. bounds in net/mac80211/scan.c:364:4 [83.964258] index 0 is out of range for type 'struct ieee80211_channel *' [83.964269] dump_stack_lvl+0x3f/0xc0 [83.964274] __ubsan_handle_out_of_bounds+0xec/0x110 [83.964281] __ieee80211_start_scan+0x601/0x990 [83.964291] nl80211_trigger_scan+0x874/0x990 [83.964298] genl_rcv_msg+0x240/0x270 [...] [1] https://bugzilla.kernel.org/show_bug.cgi?id=21881
CVE-2024-41072	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: wext: add extra SIOCSIWSCAN add extra check whether number of channels passed via 'ioctl(sock, SIOCSIWSCAN, ...)' doesn't exceed IW_MAX_CHANNELS with -EINVAL otherwise.
CVE-2024-41073	In the Linux kernel, the following vulnerability has been resolved: nvme: avoid double free special payload If a device may fail before a new special payload is added, a double free will result. Clear the RQF_SPECIAL_LOAD when the device fails.
CVE-2024-41074	In the Linux kernel, the following vulnerability has been resolved: cache/files: Set object to close if ondemand_id < 0 the user mode, it may delete the request corresponding to the random id. And the request may have not been read yet the open request will be done with the still reopen state in above case. As a result, the request corresponding to this function, so the read request is never completed and blocks other process. Fix this issue by simply set object to close if ondemand_id < 0.
CVE-2024-41075	In the Linux kernel, the following vulnerability has been resolved: cache/files: add consistency check for copen/creat completing random copen/creat requests and crashing the system. Added checks are listed below: * Generic, copen/creat can only complete read requests. * For copen, ondemand_id must not be 0, because this indicates that the request has the object corresponding to fd and req should be the same.
CVE-2024-41076	In the Linux kernel, the following vulnerability has been resolved: NFSv4: Fix memory leak in nfs4_set_security_label time we set a security xattr.
CVE-2024-41077	In the Linux kernel, the following vulnerability has been resolved: null_blk: fix validation of block size Block size must be a power of 2. The current check does not validate this, so update the check. Without this patch, null_blk would crash with bs=1536 [1]. [axboe: remove unnecessary braces and != 0 check]
CVE-2024-41078	In the Linux kernel, the following vulnerability has been resolved: btrfs: qgroup: fix quota root leak after quota disk fail when cleaning the quota tree or when deleting the root from the root tree, we jump to the 'out' label without even resulting in a leak of the root since fs_info->quota_root is no longer pointing to the root (we have set it to NULL just doing a btrfs_put_root() call under the 'out' label. This is a problem that exists since qgroups were first added in 2017 implementation and prototypes"), but back then we missed a kfree on the quota root and free_extent_buffer() calls then roots were not yet reference counted.
CVE-2024-41079	In the Linux kernel, the following vulnerability has been resolved: nvmet: always initialize cq.e.result The spec does not (aka results) for the command queue entry need to be set to 0 when they are not used (not specified). Though, the target but not for RDMA. Let's make RDMA behave the same and thus explicitly initializing the result field. This prevents the possibility of a deadlock.
CVE-2024-41080	In the Linux kernel, the following vulnerability has been resolved: io_uring: fix possible deadlock in io_register_io_uring io_register_iowq_max_workers() function calls io_put_sq_data(), which acquires the sqd->lock without releasing the lock (io_uring: drop ctx->uring_lock before acquiring sqd->lock"), this can lead to a potential deadlock if the lock is released before calling io_put_sq_data(), and then it is re-acquired after the function call. This change ensures that preventing the possibility of a deadlock.
CVE-2024-41081	In the Linux kernel, the following vulnerability has been resolved: ila: block BH in ila_output() As explained in commit 8b0e0e0e ("net/core/dst_cache.c helpers need to be called with BH disabled. ila_output() is called from process context, and under rcu_read_lock(). We might be interrupted by a softirq, re-enter ila_output() and corrupt dst_cache local_bh_disable().

CVE-2024-41082	In the Linux kernel, the following vulnerability has been resolved: nvme-fabrics: use reserved tag for reg read/write commands are issued by nvme command in the same time by user tasks, this may exhaust all tags of admin_q. If a before these commands finish, reconnect routine may fail to update nvme regs due to insufficient tags, which will cause workaround this issue, maybe we can let reg_read32()/reg_read64()/reg_write32() use reserved tags. This maybe safe will not issue connect command 2. For the enable ctrl / fw activate path, since connect and reg_xx() are called serially while reg_xx() use reserved tags.
CVE-2024-41087	In the Linux kernel, the following vulnerability has been resolved: ata: libata-core: Fix double free on error If e.g. t fails, we will jump to the err_out label, which will call devres_release_group(). devres_release_group() will trigger ata_host_release() calls kfree(host), so executing the kfree(host) in ata_host_alloc() will lead to a double free: kernel oopcode: 0000 [#1] PREEMPT SMP NOPTI CPU: 11 PID: 599 Comm: (udev-worker) Not tainted 6.10.0-rc5 #47 Hw: + PIIX, 1996), BIOS 1.16.3-2.fc40 04/01/2014 RIP: 0010:kfree+0x2cf/0x2f0 Code: 5d 41 5e 41 5f 5d e9 80 d6 ff f8 89 da RSP: 0018:ffffc90000f377f0 EFLAGS: 00010246 RAX: ffff888112b1f2c0 RBX: ffff888112b1f2c0 RCX: ffff888112b1f2c0 RSI: ffffffff02c9de5 RDI: ffff888112b1f2c0 RBP: ffff888112b1f2c0 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffea00044ac780 R13: ffff888100046400 R14: ffffffffc02c9de5 R15: 0000000000000000 GS:ffff88813b380000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CRO: 0000000008005003 CR2: 0000000011724000 CR4: 0000000000750ef0 PKRU: 55555554 Call Trace: <TASK> ? __die_body.cold+0x19/0xa do_error_trap+0x6a/0x90 ? kfree+0x2cf/0x2f0 ? exc_invalid_op+0x50/0x70 ? kfree+0x2cf/0x2f0 ? asm_exc_invalid+0xf5/0x120 [libata] ? ata_host_alloc+0xf5/0x120 [libata] ? kfree+0x2cf/0x2f0 ata_host_alloc+0xf5/0x120 [libata] ahci_init_one+0x6c9/0xd20 [ahci] Ensure that we will not call kfree(host) twice, by performing the kfree() only if
CVE-2024-41088	In the Linux kernel, the following vulnerability has been resolved: can: mcp251xfd: fix infinite loop when xmit fails function fails, the driver stops processing messages, and the interrupt routine does not return, running indefinitely Error messages: [441.298819] mcp251xfd spi.2.0 can0: ERROR in mcp251xfd_start_xmit: -16 [441.306498] mcp buffer not empty. (seq=0x000017c7, tef_tail=0x000017cf, tef_head=0x000017d0, tx_head=0x000017d3). ... and re when multiple devices share the same SPI interface. And there is concurrent access to the bus. The problem occurs mcp251xfd_start_xmit() fails. Consequently, the driver skips one TX package while still expecting a response in message issue by starting a workqueue to write the tx obj synchronously if err = -EBUSY. In case of another error, decrement stack, and drop the message. [mkl: use more imperative wording in patch description]
CVE-2024-41089	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau/dispnv04: fix null pointer dereference nv17_tv_get_hd_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference in drm_mode_duplicate(). The same applies to drm_cvt_mode(). Add a check to avoid null pointer dereference.
CVE-2024-41092	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gt: Fix potential UAF by revoke of fence reporting the following issue triggered by igt@i915_selftest@live@hangcheck on ADL-P and similar machines: intel_hangcheck_live_selftests/igt_reset_evict_fence ... i915 0000:00:02:0. [drm] GT0: GUC: SLPC enabled [414.070354] Unable to pin Y-tiled fence; err:-4 GEM_BUG_ON(!i915_active_is_idle(&fence->active)) ... gputracer: gputracer.c:301! Comm: kworker/u64:3 Tainted: G U W 6.9.0-CI_DRM_14785-g1ba62f8cea9c#1 Platform/AlderLake-P DDR4 RVP, BIOS RPLPFWI1.R00.4035.A00.2301200723 01/20/2023 [i915] [609.604149] RIP: 0010:i915_vma_revoke_fence+0x187/0x1f0 [i915] ... [609.604711] Call Trace: [609.604716] __i915_vma_evict+0x2e9/0x550 [i915] [609.604852] __i915_vma_unbind+0x7c/0x160 [i915] [609.605098] i915_vma_destroy+0x2f/0xa0 [i915] [609.605210] __i915_gem_object_pin+0x24/0xa0 [i915] [609.605210] i915_vma_destroy+0x2f/0xa0 [i915] [609.605330] __i915_gem_free_objects.isra.0+0x6a/0xc0 [i915] [609.605440] process_scheduled_works+0x11/0x20 [kworker] similar failures reported by CI from other IGT tests, observed on other platforms. Before commit 63baf4fd3d587 ("c before unbinding a GGTT fence"), i915_vma_revoke_fence() was waiting for idleness of vma->active via fence_update() before unbinding a GGTT fence. After commit 63baf4fd3d587, i915_vma_revoke_fence() would wait for vma->active to become inactive in order for the fence_update() to be able to wait selectively on that one instead of vma->active since only i915_vma_revoke_fence() could make vma->active inactive. Then, another commit 0d86ee35097a ("drm/i915/gt: Make fence revocation unequivocal") replaced the call to fence_update() with only fence_write(), and also added that GEM_BUG_ON(!i915_active_is_idle(&fence->active)) in front. No j might then expect idleness of vma->fence->active without first waiting on it. The issue can be potentially caused by registers on one side and sequential execution of signal callbacks invoked on completion of a request that was using parallel to revocation of those fence registers. Fix it by waiting for idleness of vma->fence->active in i915_vma_revoke_fence(). 24bb052d3dd499c5956abad5f7d8e4fd07da7fb1)
CVE-2024-41093	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: avoid using null object of framebuffer directly, get object from framebuffer by calling drm_gem_fb_get_obj() and return error code when object is null to
CVE-2024-41095	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau/dispnv04: fix null pointer dereference nv17_tv_get_ld_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference in drm_mode_duplicate(). Add a check to avoid npd.

CVE-2024-41097	In the Linux kernel, the following vulnerability has been resolved: usb: atm: cxacru: fix endpoint checking in cxacru an old issue [1] that occurs due to incomplete checking of present usb endpoints. As such, wrong endpoints types n in turn triggers a warning in usb_submit_urb(). Fix the issue by verifying that required endpoint types are present f account cmd endpoint type. Unfortunately, this patch has not been tested on real hardware. [1] Syzbot report: usb 1 WARNING: CPU: 0 PID: 8667 at drivers/usb/core/urb.c:502 usb_submit_urb+0xed2/0x18a0 drivers/usb/core/urb.c:502 ... Comm: kworker/0:4 Not tainted 5.14.0-rc4-syzkaller #0 Hardware name: Google Google Compute Engine/Google Workqueue: usb_hub_wq hub_event RIP: 0010:usb_submit_urb+0xed2/0x18a0 drivers/usb/core/urb.c:502 ... Call atm/cxacru.c:649 cxacru_card_status+0x22/0xd0 drivers/usb/atm/cxacru.c:760 cxacru_bind+0x7ac/0x11a0 drivers +0x321/0x1ae0 drivers/usb/atm/usbatm.c:1055 cxacru_usb_probe+0xdf/0x1e0 drivers/usb/atm/cxacru.c:1363 usb core/driver.c:396 call_driver_probe drivers/base/dd.c:517 [inline] really_probe+0x23c/0xcd0 drivers/base/dd.c:595 drivers/base/dd.c:747 driver_probe_device+0x4c/0x1a0 drivers/base/dd.c:777 __device_attach_driver+0x20b/0x2f +0x15f/0x1e0 drivers/base/bus.c:427 __device_attach+0x228/0x4a0 drivers/base/dd.c:965 bus_probe_device+0x1 +0xc2f/0x2180 drivers/base/core.c:3354 usb_set_configuration+0x113a/0x1910 drivers/usb/core/message.c:2170 u drivers/usb/core/generic.c:238 usb_probe_device+0xd9/0x2c0 drivers/usb/core/driver.c:293
CVE-2024-41098	In the Linux kernel, the following vulnerability has been resolved: ata: libata-core: Fix null pointer dereference on ata_host_alloc() fails, ata_host_release() will get called. However, the code in ata_host_release() tries to free ata_p can lead to the following: BUG: unable to handle page fault for address: 0000000000003990 PGD 0 P4D 0 Oops: CPU: 10 PID: 594 Comm: (udev-worker) Not tainted 6.10.0-rc5 #44 Hardware name: QEMU Standard PC (i440FX 04/01/2014 RIP: 0010:ata_host_release.cold+0x2f/0x6e [libata] Code: e4 4d 63 f4 44 89 e2 48 c7 c6 90 ad 32 c0 4 0018:ffffc90000ebb968 EFLAGS: 00010246 RAX: 0000000000000041 RBX: ffff88810fb52e78 RCX: 00000000 RSI: ffff88813b3218c0 RDI: ffff88813b3218c0 RBP: ffff88810fb52e40 R08: 0000000000000000 R09: 6c65725f7 73692033203a746e R12: 0000000000000004 R13: 0000000000000000 R14: 0000000000000011 R15: 0000000000000000 GS:ffff88813b300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 C 00000001122a2000 CR4: 0000000000750ef0 PKRU: 55555554 Call Trace: <TASK> ? __die_body.cold+0x19/0x exc_page_fault+0x7e/0x180 ? asm_exc_page_fault+0x26/0x30 ? ata_host_release.cold+0x2f/0x6e [libata] ? ata_h release_nodes+0x35/0xb0 devres_release_group+0x113/0x140 ata_host_alloc+0xed/0x120 [libata] ata_host_alloc +0xc69/0xd20 [ahci] Do not access ata_port struct members unconditionally.
CVE-2024-42063	In the Linux kernel, the following vulnerability has been resolved: bpf: Mark bpf prog stack with kmsan_unposion reported uninit memory usages during map_{lookup,delete}_elem. ===== BUG: KMSAN: uninit-value in devmap.c:441 [inline] BUG: KMSAN: uninit-value in dev_map_lookup_elem+0xf3/0x170 kernel/bpf/devmap.c:7 bpf/devmap.c:441 [inline] dev_map_lookup_elem+0xf3/0x170 kernel/bpf/devmap.c:796 ____bpf_map_lookup_el bpf_map_lookup_elem+0x5c/0x80 kernel/bpf/helpers.c:38 ____bpf_prog_run+0x13fe/0xe0f0 kernel/bpf/core.c:199 bpf/core.c:2237 ===== The reproducer should be in the interpreter mode. The C reproducer is trying to run (18) r1 = map[id:49] 4: (b7) r8 = 16777216 5: (7b) *(u64 *) (r10 -8) = r8 6: (bf) r2 = r10 7: (07) r2 += -229 ^^^^^ dev_map_lookup_elem#1543472 11: (95) exit It is due to the "void *key" (r2) passed to the helper. bpf allows unin the right privileges. This patch uses kmsan_unpoison_memory() to mark the stack as initialized. This should addre *key" argument during map_{lookup,delete}_elem.
CVE-2024-42064	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Skip pipe if the pipe idx not s idx not set properly [how] Add code to skip the pipe that idx not set properly
CVE-2024-42065	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Add a NULL check in xe_ttm_stolen_m the mgr is not NULL.
CVE-2024-42066	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix potential integer overflow in page s >page_alignment to u64 before bit-shifting to prevent overflow when assigning to min_page_size.
CVE-2024-42067	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_rox() into ac set_memory_rox() can fail, leaving memory unprotected. Check return and bail out when bpf_jit_binary_lock_ro()
CVE-2024-42068	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_ro() into acc set_memory_ro() can fail, leaving memory unprotected. Check its return and take it into account as an error.
CVE-2024-42070	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fully validate NFT_DATA_ store validation for NFT_DATA_VALUE is conditional, however, the datatype is always either NFT_DATA_VAL requires a new helper function to infer the register type from the set datatype so this conditional check can be remo leaked through the registers.

CVE-2024-42076	In the Linux kernel, the following vulnerability has been resolved: net: can: j1939: Initialize unused data in j1939_... in raw_recvmsg() [1]. j1939_send_one() creates full frame including unused data, but it doesn't initialize it. This can be fixed by initializing unused data. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumentation.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 [inline] instrumented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] iterate_ubuf include/linux/iov_iter.h:29 [inline] iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline] _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 [inline] linux/uio.h:196 [inline] memcpy_to_msg include/linux/skbuff.h:4113 [inline] raw_recvmsg+0x2b8/0x9e0 net/can/raw_sock.c:1046 [inline] sock_recvmsg+0x2c4/0x340 net/socket.c:1068 ____sys_recvmsg+0x18a/0x620 net/socket.c:2845 do_recvmsg+0x4fc/0xfd0 net/socket.c:2939 ____sys_recvmsg net/socket.c:3018 [inline] __do_sys_recvmsg net/socket.c:3034 [inline] __x64_sys_recvmsg+0x397/0x490 net/socket.c:3034 x64/include/generated/asm/syscalls_64.h:300 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xc0/0x100 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inline] kmem_cache_alloc_node+0x613/0xc50 mm/slub.c:3888 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:658 skbbuf.c:668 alloc_skb include/linux/skbuff.h:1313 [inline] alloc_skb_with_fragments+0xc8/0xbf0 net/core/skbuff.c:658 core/sock.c:2795 sock_alloc_send_skb include/net/sock.h:1842 [inline] j1939_sk_alloc_skb net/can/j1939/socket.c:1142 [inline] j1939_sk_sendmsg+0xc0a/0x2730 net/can/j1939/socket.c:1277 sock_sendmsg_nosec+0x30f/0x380 net/socket.c:745 ____sys_sendmsg+0x877/0xb60 net/socket.c:2584 __sys_sendmsg+0x28d/0x3c0 net/socket.c:2667 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] do_syscall_x64 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Bytes 12 of size 16 starts at ffff888120969690 Data copied to user address 00000000200017c0 CPU: 1 PID: 5050 Comm: syzkaller-00031-g71b1543c83d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:__xdp_reg_mem_model+0x22/0x40 net/core/xdp.c:344 xdp_test_run_setup net/bpf/test_run.c:188 [inline] bpf_test_run+0x377/0x3ff bpf_prog_test_run_xdp+0x813/0x11b0 net/bpf/test_run.c:1267 bpf_prog_test_run+0x33a/0x3b0 net/bpf/test_run.c:364 [inline] kernel/bpf/syscall.c:5649 __do_sys_bpf kernel/bpf/syscall.c:5738 [inline] __se_sys_bpf kernel/bpf/syscall.c:5736 do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x6d/0x75 (linuxtesting.org) with syzkaller.
CVE-2024-42077	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix DIO failure due to insufficient transaction credits using ocfs2_calc_extend_credits(). The ocfs2_dio_end_io_write() estimates number of necessary transaction credits using ocfs2_calc_extend_credits(). That means that the IO could be arbitrarily large and can contain arbitrary number of extents. Extent tree manipulations do often happen in all of the cases. For example if we have only single block extents in the tree, ocfs2_mark_extent_written() will extend all the time and we will never extend the current transaction and eventually exhaust all the transaction credits if the extent tree grows too big. Once that happens a WARN_ON(jbd2_handle_buffer_credits(handle) <= 0) is triggered in jbd2_journal_dirty_metadata() in response to this error. This was actually triggered by one of our customers on a heavily fragmented OCFS2 filesystem. Transaction always has enough credits for one extent insert before each call of ocfs2_mark_extent_written(). Hemingway - not syncing: OCFS2: (device dm-1): panic forced after error" PID: xxx TASK: xxxx CPU: 5 COMMAND: "Subprocess" ffffffff8c069932 #1 __crash_kexec at ffffffff8c1338fa #2 panic at ffffffff8c1d69b9 #3 ocfs2_handle_error at ffffffffb0c88387 [ocfs2] #5 ocfs2_journal_dirty at ffffffffb0c51e98 [ocfs2] #6 ocfs2_split_extent at ffffffffb0c27ea2 [ocfs2] #7 ocfs2_mark_extent_written at ffffffffb0c28347 [ocfs2] #9 ocfs2_dio_end_io_write at ffffffffb0c2c0f5 [ocfs2] #11 dio_complete at ffffffffb0c2b9fa7 #12 do_blockdev_direct_IO at ffffffffb0c2bc09f #13 generic_file_direct_write at ffffffffb0c1dcf14 #15 __generic_file_write_iter at ffffffffb0c1dd07b #16 ocfs2_file_aio_write at ffffffffb0c2cc72e #18 kmem_cache_alloc at ffffffffb0c248dde #19 do_io_submit at ffffffffb0c2ccada #20 entry_SYSCALL_64_after_hwframe at ffffffffb0c8000ba
CVE-2024-42079	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix NULL pointer dereference in gfs2_log_flush(). In gfs2_log_flush(), check if log_flush_lock is held under the log flush lock to provide exclusion against gfs2_log_flush(). Otherwise, we could run into a NULL pointer dereference when outstanding glock work races with log_flush_queue -> inode_xmote -> inode_go_sync -> gfs2_log_flush).
CVE-2024-42080	In the Linux kernel, the following vulnerability has been resolved: RDMA/restrack: Fix potential invalid address access in rdma_restrack_clean() when print the owner of this rdma_restrack_entry. These code is used to help find one for free is not needed anymore, so delete them.
CVE-2024-42081	In the Linux kernel, the following vulnerability has been resolved: drm/xe/xe_devcoredump: Check NULL before accessing 'xe_devcoredump_snapshot' and 'xe_device' *only if 'coredump' is not NULL. v2 - Fix commit messages. v3 - Drop return check for coredump_to_xe. (Jose/Rodrigo) v5 - Modify misleading commit message. (Matt)
CVE-2024-42082	In the Linux kernel, the following vulnerability has been resolved: xdp: Remove WARN() from __xdp_reg_mem_model(). The warning occurs only if __mem_id_init_hash_table() returns an error. It returns the error if 1. rhashtable_init() fails; 2. rhashtable_init() fails when some fields of rhashtable_params struct are not initialized properly. The second static const rhashtable_params struct with valid fields. So, warning is only triggered when there is a problem with the sense in using WARN() to handle this error and it can be safely removed. WARNING: CPU: 0 PID: 5065 at net/core/xdp.c:299 xdp_test_run_setup net/bpf/test_run.c:188 [inline] bpf_test_run+0x377/0x3ff bpf_prog_test_run_xdp+0x813/0x11b0 net/bpf/test_run.c:1267 bpf_prog_test_run+0x33a/0x3b0 net/bpf/test_run.c:364 [inline] kernel/bpf/syscall.c:5649 __do_sys_bpf kernel/bpf/syscall.c:5738 [inline] __se_sys_bpf kernel/bpf/syscall.c:5736 do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x6d/0x75 (linuxtesting.org) with syzkaller.

CVE-2024-42084	In the Linux kernel, the following vulnerability has been resolved: ftruncate: pass a signed offset The old ftruncate extension when called in compat mode on 64-bit architectures. As a result, passing a negative length accidentally set 2GiB and 4GiB. Changing the type of the compat syscall to the signed compat_off_t changes the behavior so it isn't the truncate() syscall and the corresponding loff_t based variants are all correct already and do not suffer from this
CVE-2024-42086	In the Linux kernel, the following vulnerability has been resolved: iio: chemical: bme680: Fix overflows in compensate functions of the driver that there could be overflows of variables due to bit shifting ops. These implications they were mentioned in log message of Commit 1b3bd8592780 ("iio: chemical: Add support for Bosch BME680 sensor") iio/20180728114028.3c1bbe81@archlinux/
CVE-2024-42087	In the Linux kernel, the following vulnerability has been resolved: drm/panel: ilitek-ili9881c: Fix warning with GPIO controls the reset GPIO using the non-sleeping gpiod_set_value() function. This complains loudly when the GPIO is asleep, use gpiod_set_value_cansleep() to fix the issue.
CVE-2024-42089	In the Linux kernel, the following vulnerability has been resolved: ASoC: fsl-asoc-card: set priv->pdev before using being used in fsl_asoc_card_audmux_init(). Move this assignment at the start of the probe function, so sub-function fsl_asoc_card_audmux_init() dereferences priv->pdev to get access to the dev struct, used with dev_err macros. As NULL pointer dereference. Note that if priv->dev is dereferenced before assignment but never used, for example if won't crash probably due to compiler optimisations.
CVE-2024-42090	In the Linux kernel, the following vulnerability has been resolved: pinctrl: fix deadlock in create_pinctrl() when has pinctrl_maps_mutex is acquired before calling add_setting(). If add_setting() returns -EPROBE_DEFER, create_pinctrl_free() attempts to acquire pinctrl_maps_mutex, which is already held by create_pinctrl(), leading to a potential deadlock by releasing pinctrl_maps_mutex before calling pinctrl_free(), preventing the deadlock. This bug was discovered at Security Testing (SAST) by Synopsys, Inc.
CVE-2024-42091	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Check pat.ops before dumping PAT settings running on brand new platform or when running as a VF. While the former is unlikely, the latter is valid (future) use will try to dump PAT settings by debugfs. It's better to check pointer to pat.ops instead of specific .dump hook, as it's every .ops variant.
CVE-2024-42092	In the Linux kernel, the following vulnerability has been resolved: gpio: davinci: Validate the obtained number of IRQs from Device Tree. In case of broken DT due to any error this value can be any. Without this value validation there is an access in davinci_gpio_probe(). Validate the obtained nrirq value so that it won't exceed the maximum number of IRQs. Center (linuxtesting.org) with SVACE.
CVE-2024-42093	In the Linux kernel, the following vulnerability has been resolved: net/dpaa2: Avoid explicit cpumask var allocation CONFIG_CPUMASK_OFFSTACK=y kernel, explicit allocation of cpumask variable on stack is not recommended due to stack overflow. Instead, kernel code should always use *cpumask_var API(s) to allocate cpumask var in config-neutral way CONFIG_CPUMASK_OFFSTACK. Use *cpumask_var API(s) to address it.
CVE-2024-42094	In the Linux kernel, the following vulnerability has been resolved: net/iucv: Avoid explicit cpumask var allocation CONFIG_CPUMASK_OFFSTACK=y kernel, explicit allocation of cpumask variable on stack is not recommended due to stack overflow. Instead, kernel code should always use *cpumask_var API(s) to allocate cpumask var in config-neutral way CONFIG_CPUMASK_OFFSTACK. Use *cpumask_var API(s) to address it.
CVE-2024-42095	In the Linux kernel, the following vulnerability has been resolved: serial: 8250_omap: Implementation of Errata i2012 timeout can be triggered, if this Erroneous interrupt is not cleared then it may leads to storm of interrupts, therefore www.ti.com/lit/pdf/sprz536 page 23
CVE-2024-42096	In the Linux kernel, the following vulnerability has been resolved: x86: stop playing stack games in profile_pc() The timer-based profiling, which isn't really all that relevant any more to begin with, but it also ends up making assumptions necessarily valid. Basically, the code tries to account the time spent in spinlocks to the caller rather than the spinlock not worth the code complexity or the KASAN warnings when no serious profiling is done using timers anyway the stack layout that is only true in the simplest of cases. We've lost the comment at some point (I think when the 32-bit to say: Assume the lock function has either no stack frame or a copy of eflags from PUSHF. which explains why it off the stack pointer and then takes a minimal look at the values to just check if they might be eflags or the return pointer unlike kernel addresses but that basic stack layout assumption assumes that there isn't any lock debugging etc going a stack frame. It causes KASAN unhappiness reported for years by syzkaller [1] and others [2]. With no real practice the code. Just for historical interest, here's some background commits relating to this code from 2006: 0cb91a22936 ("during profiling for !FP kernels") 31679f38d886 ("Simplify profile_pc on x86-64") and a code unification from 2006: profile_pc") but the basics of this thing actually goes back to before the git tree.
CVE-2024-42097	In the Linux kernel, the following vulnerability has been resolved: ALSA: emux: improve patch ioctl data validation skipping over the main info block match that in load_guspitch(). In load_guspitch(), add checking that the specified data, like load_data() already did.
CVE-2024-42098	In the Linux kernel, the following vulnerability has been resolved: crypto: ecdh - explicitly zeroize private_key parameter passed in by the caller (if present), or alternatively a newly generated private key. However, it is possible to generate a key (generated key) which is shorter than the previous key. In that scenario, some key material from the previous key would be left in the private_key array. This patch slightly changes the behavior of this function: if the key failed, the old private_key would remain. Now, the private_key is always zeroized. This behavior is consistent with ecc_is_key_valid fails.

CVE-2024-42101	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau: fix null pointer dereference in nouveau_connector_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to failure of drm_mode_duplicate(). Add a check to avoid npd.
CVE-2024-42102	In the Linux kernel, the following vulnerability has been resolved: Revert "mm/writeback: fix possible divide-by-zero in mm: Avoid possible overflows in dirty throttling". Dirty throttling logic assumes dirty limits in page units fit into true (see patch 2/2 for more details). This patch (of 2): This reverts commit 9319b647902cbd5cc884ac08a8a6d54c ways. Firstly, the removed (u64) cast from the multiplication will introduce a multiplication overflow on 32-bit architectures is actually common - the default settings with 4GB of RAM will trigger this). Secondly, the div64_u64() is unnecessary, div64_ul() in case we want to be safe & cheap. Thirdly, if dirty thresholds are larger than 1<<32 pages, then dirty bytes in spectacular ways anyway so trying to fix one possible overflow is just moot.
CVE-2024-42104	In the Linux kernel, the following vulnerability has been resolved: nilfs2: add missing check for inode numbers on mounting and unmounting a specific pattern of corrupted nilfs2 filesystem images causes a use-after-free of metadata lru_add_fn(). As Jan Kara pointed out, this is because the link count of a metadata file gets corrupted to 0, and nilfs2 tries to delete that inode (ifile inode in this case). The inconsistency occurs because directories containing the inodes not be visible in the namespace are read without checking. Fix this issue by treating the inode numbers of these inodes when reading directory folios/pages. Also thanks to Hilf Danton and Matthew Wilcox for their initial mm-layer analysis.
CVE-2024-42105	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix inode number range checks Patch series "to reserved inodes". This series fixes one use-after-free issue reported by syzbot, caused by nilfs2's internal inode block in corrupted filesystem, and a couple of flaws that cause problems if the starting number of non-reserved inodes written (or corruptly) changed from its default value. This patch (of 3): In the current implementation of nilfs2, "nilfs->ns_reserved_inode_number", is read from the superblock, but its lower limit is not checked. As a result, if a number that is out of reserved inodes such as the root directory or metadata files is set in the super block parameter, the inode number (NILFS_VALID_INODE) will not function properly. In addition, these test macros use left bit-shift calculations using the BIT macro, but the result of a shift calculation that exceeds the bit width of an integer is undefined in the C standard. If a large value other than the default value NILFS_USER_INO (=11), the macros may potentially malfunction depending on the compiler by checking the lower bound of "nilfs->ns_first_ino" and by preventing bit shifts equal to or greater than the NILFS test macros. Also, change the type of "ns_first_ino" from signed integer to unsigned integer to avoid the need for type bound check introduced this time.
CVE-2024-42106	In the Linux kernel, the following vulnerability has been resolved: inet_diag: Initialize pad field in struct inet_diag_req_v2 value access in raw_lookup() [1]. Diag for raw sockets uses the pad field in struct inet_diag_req_v2 for the underlying protocol to the sdiag_raw_protocol field in struct inet_diag_req_raw. inet_diag_get_exact_compat() converts inet_diag_req_v2 to the pad field uninitialized. So the issue occurs when raw_lookup() accesses the sdiag_raw_protocol field. Fix this by initializing the pad field in inet_diag_get_exact_compat(). Also, do the same fix in inet_diag_dump_compat() to avoid the similar issue in the dump path. [1] raw_lookup net/ipv4/raw_diag.c:49 [inline] BUG: KMSAN: uninit-value in raw_sock_get+0x657/0x800 net/ipv4/raw_sock.c:49 [inline] raw_sock_get+0x657/0x800 net/ipv4/raw_diag.c:71 raw_diag_dump_one+0xa1/0x660 net/ipv4/raw_diag.c:1404 [inline] inet_diag_rcv_msg_compat+0x469/0x530 net/core/sock_diag.c:282 netlink_rcv_skb+0x537/0x670 net/netlink/af_netlink.c:1335 [inline] netlink_unicast_kernel net/netlink/af_netlink.c:1335 [inline] netlink_unicast+0xe74/0x1240 net/netlink/af_netlink.c:1905 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg net/socket.c:2639 [inline] __do_sys_sendmsg net/socket.c:2677 [inline] __se_sys_sendmsg net/socket.c:2675 [inline] __x64_sys_sendmsg+0xc6/0x135e arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/common.c:52 [inline] entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was stored to memory at: raw_sock_get+0xa1/0x660 net/ipv4/raw_diag.c:99 inet_diag_cmd_exact+0x7d9/0x980 inet_diag_get_exact+0x469/0x530 net/ipv4/inet_diag.c:1426 sock_diag_rcv_msg+0x23d/0x740 net/core/sock_diag.c:297 netlink_unicast_kernel net/netlink/af_netlink.c:1335 [inline] netlink_unicast+0xe74/0x1240 net/netlink/af_netlink.c:1361 netlink_sendmsg+0x10c6/0x1260 net/netlink/af_netlink.c:1361 [inline] __sock_sendmsg+0x332/0x3d0 net/socket.c:745 __sys_sendmsg+0x7f0/0xb70 net/socket.c:2639 [inline] __do_sys_sendmsg net/socket.c:2668 [inline] __se_sys_sendmsg net/socket.c:2677 [inline] __x64_sys_sendmsg+0xc6/0x135e arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/common.c:52 [inline] entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was stored to memory at: inet_diag_get_exact_compat net/ipv4/inet_diag.c:1396 [inline] inet_diag_rcv_msg_compat net/netlink/af_netlink.c:1426 sock_diag_rcv_msg+0x23d/0x740 net/core/sock_diag.c:282 CPU: 1 PID: 8888 Comm: syz-executor.6 Not tainted Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-2.fc40 04/01/2014

CVE-2024-42110	<p>In the Linux kernel, the following vulnerability has been resolved: net: ntb_netdev: Move ntb_netdev_rx_handler()</p> <p>The following is emitted when using idxd (DSA) dmanegine as the data mover for ntb_transport that ntb_netdev uses smp_processor_id() in preemptible [00000000] code: irq/52-idxd-por/14526 [74412.556784] caller is netif_rx_inte CPU: 6 PID: 14526 Comm: irq/52-idxd-por Not tainted 6.9.5 #5 [74412.569870] Hardware name: Intel Corporation EGSDCRB1.E91.1752.P05.2402080856 02/08/2024 [74412.581699] Call Trace: [74412.584514] <TASK> [74412.591129] check_preemption_disabled+0xc8/0xf0 [74412.596374] netif_rx_internal+0x42/0x130 [74412.60 ntb_netdev_rx_handler+0x66/0x150 [ntb_netdev] [74412.610985] ntb_complete_rxc+0xed/0x140 [ntb_transport] +0x53/0x80 [ntb_transport] [74412.623332] idxd_dma_complete_tx+0xe3/0x160 [idxd] [74412.628963] idxd_w irq_thread_fn+0x21/0x60 [74412.638134] ? irq_thread+0xa8/0x290 [74412.642218] irq_thread+0x1a0/0x290 [744 +0x10/0x10 [74412.651071] ? __pfx_irq_thread_dtor+0x10/0x10 [74412.656117] ? __pfx_irq_thread+0x10/0x10 [74412.664384] ? __pfx_kthread+0x10/0x10 [74412.668639] ret_from_fork+0x31/0x50 [74412.672716] ? __pfx ret_from_fork_asm+0x1a/0x30 [74412.681457] </TASK> The cause is due to the idxd driver interrupt completion threaded handler is not hard or soft interrupt context. However __netif_rx() can only be called from interrupt context to allow completion via normal context for dmaengine drivers that utilize threaded irq handling. While the following __netif_rx(), baebdf48c360 ("net: dev: Makes sure netif_rx() can be invoked in any context."), the change should've precedes this fix should've been using netif_rx_ni() or netif_rx_any_context().</p>
CVE-2024-42114	<p>In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: restrict NL80211_ATTR_TXQ trigger softlockups, setting NL80211_ATTR_TXQ_QUANTUM to 2^31. We had a similar issue in sch_fq, fixed with fq: do not accept silly TCA_FQ_QUANTUM") watchdog: BUG: soft lockup - CPU#1 stuck for 26s! [kworker/1:0:131135 hardirqs last enabled at (131134): [<ffff80008ae8778c>] __exit_to_kernel_mode arch/arm64/kernel/entry-common.c: [74412.556784] caller is netif_rx_inte CPU: 6 PID: 14526 Comm: irq/52-idxd-por Not tainted 6.9.5 #5 [74412.569870] Hardware name: Intel Corporation EGSDCRB1.E91.1752.P05.2402080856 02/08/2024 [74412.581699] Call Trace: [74412.584514] <TASK> [74412.591129] check_preemption_disabled+0xc8/0xf0 [74412.596374] netif_rx_internal+0x42/0x130 [74412.60 ntb_netdev_rx_handler+0x66/0x150 [ntb_netdev] [74412.610985] ntb_complete_rxc+0xed/0x140 [ntb_transport] +0x53/0x80 [ntb_transport] [74412.623332] idxd_dma_complete_tx+0xe3/0x160 [idxd] [74412.628963] idxd_w irq_thread_fn+0x21/0x60 [74412.638134] ? irq_thread+0xa8/0x290 [74412.642218] irq_thread+0x1a0/0x290 [744 +0x10/0x10 [74412.651071] ? __pfx_irq_thread_dtor+0x10/0x10 [74412.656117] ? __pfx_irq_thread+0x10/0x10 [74412.664384] ? __pfx_kthread+0x10/0x10 [74412.668639] ret_from_fork+0x31/0x50 [74412.672716] ? __pfx ret_from_fork_asm+0x1a/0x30 [74412.681457] </TASK> The cause is due to the idxd driver interrupt completion threaded handler is not hard or soft interrupt context. However __netif_rx() can only be called from interrupt context to allow completion via normal context for dmaengine drivers that utilize threaded irq handling. While the following __netif_rx(), baebdf48c360 ("net: dev: Makes sure netif_rx() can be invoked in any context."), the change should've precedes this fix should've been using netif_rx_ni() or netif_rx_any_context().</p>
CVE-2024-42115	<p>In the Linux kernel, the following vulnerability has been resolved: jffs2: Fix potential illegal address access in jffs2 jffs2 file system, the following abnormal printouts were found: [2430.649000] Unable to handle kernel paging request [2430.649622] Mem abort info: [2430.649829] ESR = 0x96000004 [2430.650115] EC = 0x25: DABT (current EL0) [2430.650795] EA = 0, S1PTW = 0 [2430.651032] FSC = 0x04: level 0 translation fault [2430.651446] = 0x00000004 [2430.652001] CM = 0, WnR = 0 [2430.652558] [0069696969696948] address between user and kernel error: Oops: 96000004 [#1] PREEMPT SMP [2430.654512] CPU: 2 PID: 20919 Comm: cat Not tainted 5.15.25-g name: linux,dummy-virt (DT) [2430.655517] pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYP [2430.656630] lr : jffs2_free_inode+0x24/0x48 [2430.657051] sp : ffff800009eebd10 [2430.657355] x29: ffff800 0000000000000000 [2430.658327] x26: ffff000038f09d80 x25: 0080000000000000 x24: ffff800009d38000 [2430.659434] x20: ffff0000bf9a6ac0 x19: 0169696969696940 x18: 0000000000000000 x16: ffff800009e0c000 x15: 0000000000000400 [2430.660637] x14: 0000000000000000 x13: [2430.661345] x11: 0004000800000000 x10: 0000000000000001 x9: ffff8000084f0d14 [2430.662025] x8: ffff000 000000003470302 [2430.662695] x5: ffff00002e41dcc0 x4: ffff0000bf9aa3b0 x3: 0000000003470342 [2430.663375] x1: ffff8000084f0d14 x0: ffff000000000000 [2430.664217] Call trace: [2430.664528] kfree+0x78/0x348 [2430.665233] i_callback+0x24/0x50 [2430.665528] rcu_do_batch+0x1ac/0x448 [2430.665892] rcu_core+0x28 [2430.666473] __do_softirq+0x138/0x3cc [2430.666781] irq_exit+0xf0/0x110 [2430.667065] handle_irq+0xac/0xe8 [2430.667739] call_on_irq_stack+0x28/0x54 The parameter passed to kfree was 5a5a5a5a, which is the jffs_inode_info structure. It was found that all variables in the jffs_inode_info structure were 5a5a5a5a, except for these variables are not initialized because they were set to 5a5a5a5a during memory testing, which is meant to detect uninitialized variables. jffs2_i_init_once, while other members are initialized in the function jffs2_init_inode_info, is called after iget_locked, but in the iget_locked function, the destroy_inode process is triggered, which releases the member of the inode is not initialized. In concurrent high pressure scenarios, iget_locked may enter the destroy_inode functionality of jffs2 only releases the target, the fix method is to set target to NULL in jffs2_i_init_once.</p>

107

CVE-2024-42131	In the Linux kernel, the following vulnerability has been resolved: mm: avoid overflows in dirty throttling logic. The assumptions that dirty limits in PAGE_SIZE units fit into 32-bit (so that various multiplications fit into 64-bits). If overflows, possible divisions by 0 etc. Fix these problems by never allowing so large dirty limits as they have dubious dirty_background_bytes interfaces we can just refuse to set so large limits. For dirty_ratio / dirty_background_ratio computed from the amount of available memory which can change due to memory hotplug etc. So when converting, we just don't allow the result to exceed UINT_MAX. This is root-only triggerable problem which occurs when the
CVE-2024-42134	In the Linux kernel, the following vulnerability has been resolved: virtio-pci: Check if is_avq is NULL [bug] In the vp_dev->is_avq is involved to determine whether it is admin virtqueue, but this function vp_dev->is_avq may be called does not assign a value to vp_dev->is_avq. [fix] Check whether it is vp_dev->is_avq before use. [test] Test with virtio following command would crash the guest system After applying the patch, everything seems to be working fine.
CVE-2024-42135	In the Linux kernel, the following vulnerability has been resolved: vhost_task: Handle SIGKILL by flushing work. When device is closed, this has us handle SIGKILL by: 1. marking the worker as killed so we no longer try to use it with setting the virtqueue to worker mapping so no new works are queued. 3. running all the exiting works.
CVE-2024-42136	In the Linux kernel, the following vulnerability has been resolved: cdrom: rearrange last_media_change check to avoid a syzkaller with the newly reintroduced signed integer wrap sanitizer we encounter this splat: [366.015950] UBSAN: cdrom/cdrom.c:2361:33 [366.021089] -9223372036854775808 - 346321 cannot be represented in type '__s64' (aka: executor.4 is using a deprecated SCSI ioctl, please convert it to SG_IO [366.027502] CPU: 5 PID: 28472 Comm: gb3ef86b5a957 #1 [366.027512] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian Call Trace: [366.027523] <TASK> [366.027533] dump_stack_lvl+0x93/0xd0 [366.027899] handle_overflow+0x multi_count 32 ignored [366.043924] cdrom_ioctl+0x2c3f/0x2d10 [366.063932] ? __pm_runtime_resume+0xe6/ +0x15d/0x1d0 [366.074624] ? __pfx_sr_block_ioctl+0x10/0x10 [366.077642] blkdev_ioctl+0x419/0x500 [366. Historically, the signed integer overflow sanitizer did not work in the kernel due to its interaction with `fwrapv` but newest version of Clang. It was re-enabled in the kernel with Commit 557f8c582a9ba8ab ("ubsan: Reintroduce signed check to not perform any arithmetic, thus not tripping the sanitizer.
CVE-2024-42137	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: qca: Fix BT enable failure again for 272970be3dab ("Bluetooth: hci_qca: Fix driver shutdown on closed serdev") will cause below regression issue: BT boot -> enable BT -> disable BT -> warm reboot -> BT enable failure if property enable-gpios is not configured with is to fix a use-after-free issue within qca_serdev_shutdown() by adding condition to avoid the serdev is flushed or a regression issue regarding above steps since the VSC is not sent to reset controller during warm reboot. Fixed by setting qca_serdev_shutdown() once BT was ever enabled, and the use-after-free issue is also fixed by this change since then or wrote. Verified by the reported machine Dell XPS 13 9310 laptop over below two kernel commits: commit e00fcoredump implementation for QCA") of bluetooth-next tree. commit b23d98d46d28 ("Bluetooth: btusb: Fix trigger linux mainline tree.
CVE-2024-42143	In the Linux kernel, the following vulnerability has been resolved: orangefs: fix out-of-bounds fsid access Arnd Bergner "orangefs_statfs() copies two consecutive fields of the superblock into the statfs structure, which triggers a warning Kara suggested an alternate way to do the patch to make it more readable. I ran both ideas through xfstests and both suggestion.
CVE-2024-42144	In the Linux kernel, the following vulnerability has been resolved: thermal/drivers/mediatek/lvts_thermal: Check N not NULL before using it.
CVE-2024-42145	In the Linux kernel, the following vulnerability has been resolved: IB/core: Implement a limit on UMAD receive L maintains received MAD packets in an unbounded list, poses a risk of uncontrolled growth. As user-space applications of extraction may not match the rate of incoming packets, leading to potential list overflow. To address this, we introduce considering typical scenarios, such as OpenSM processing, which can handle approximately 100k packets per second packets, we set the list size limit to 200k. Packets received beyond this limit are dropped, assuming they are likely user-space. Notably, packets queued on the receive list due to reasons like timed-out sends are preserved even when
CVE-2024-42146	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Add outer runtime_pm protection to xe, doing any memory access should get their own runtime_pm outer references since they don't use the standard driver from the same driver. Found by pre-merge CI on adding WARN calls for unprotected inner callers: <6> [318.6397] xe_test_dmabuf_import_same_driver <4> [318.639957] -----[cut here]----- <4> [318.639967] xe 0000 protection <4> [318.640049] WARNING: CPU: 117 PID: 3832 at drivers/gpu/drm/xe/xe_pm.c:533 xe_pm_runtime
CVE-2024-42147	In the Linux kernel, the following vulnerability has been resolved: crypto: hisilicon/debugfs - Fix debugfs uninit probe the debugfs failure does not stop the probe. When debugfs initialization fails, jumping to the error branch will also operation. As a result, it may be released repeatedly during the regs uninit process. Therefore, the null check needs

CVE-2024-42148	In the Linux kernel, the following vulnerability has been resolved: bnx2x: Fix multiple UBSAN array-index-out-of-bounds when using a system with 32 physical cpu cores or more, or when the user defines a number of Ethernet queues greater than 16 using the num_queues module parameter. Currently there is a read/write out of bounds that occurs on the array "struct stats_query_entry query" in "drivers/net/ethernet/broadcom/bnx2x/bnx2x_stats.c". Looking at the definition of the struct stats_query_entry query[FP_SB_MAX_E1x+ BN2X2X_FIRST_QUEUE_QUERY_IDX]; FP_SB_MAX_E1x is the number of fast path interrupts and has a value of 16, while BN2X2X_FIRST_QUEUE_QUERY_IDX has a value of 3 meaning that accesses to "struct stats_query_entry query" are offset-tered by BN2X2X_FIRST_QUEUE_QUERY_IDX, that means that the array should not exceed FP_SB_MAX_E1x (16). However one of these queues is reserved for FCOE and thus the number of queues [FP_SB_MAX_E1x -1] (15) if FCOE is enabled or [FP_SB_MAX_E1x] (16) if it is not. This is also described in a comment in ethernet/broadcom/bnx2x/bnx2x.h just above the Macro definition of FP_SB_MAX_E1x. Below is the part of this comment: * The total number of L2 queues, MSIX vectors and HW contexts (CIDs) is * control by the number of fast-path status blocks (FP-SB). Each fast-path status block (FP-SB) aka non-default * status block represents an independent interrupts context for a queue. However special L2 queues such * as the FCoE queue do not require a FP-SB and other components like * as the number of possible L2 queues * * If the maximum number of FP-SB available is X then: * a. If CNIC is supported then the number of * regular L2 queues is Y=X-1 * b. In MF mode the actual number of L2 queues is Y= (X-1/MF_factor) * c. If the number of L2 queues * is Y+1 * d. The number of irq (MSIX vectors) is either Y+1 (one extra for * slow-path interrupts) or Y+2 (one extra for additional * FP interrupt context for the CNIC). * e. The number of HW context (CID count) is always X or X+1 if the FCoE L2 queue is always X. */ However this driver also supports NICs that use the E2 controller which can have a queue represented by FP_SB_MAX_E2. Looking at the commits when the E2 support was added, it was originally using a comment ("bnx2x: Add 57712 support"). Back then FP_SB_MAX_E2 was set to 16 the same as E1x. However the driver was updated to use E2 instead of having it be limited to the capabilities of the E1x. But as far as we can tell, the array "stats_query_entry" was made available to the E1x cards as part of an oversight when the driver was updated to take full advantage of the E2, and the greater queue size supported by E2 NICs, it causes the UBSAN warnings seen in the stack traces below. This patch fixes the "query" array by replacing FP_SB_MAX_E1x with FP_SB_MAX_E2 to be large enough to handle both types of NICs. The out-of-bounds in drivers/net/ethernet/broadcom/bnx2x/bnx2x_stats.c:1529:11 index 20 is out of range for type 'stats_query_entry' systemd-network Not tainted 6.9.0-060900rc7-generic #202405052133 Hardware name: HP ProLiant DL360 Gen9
CVE-2024-42151	In the Linux kernel, the following vulnerability has been resolved: bpf: mark bpf_dummy_struct_ops.test_1 parameter bpf_dummy_init_ret_value passes NULL as the first parameter of the test_1() function. Mark this parameter as nullable. Otherwise, NULL check in the test_1() code: SEC("struct_ops/test_1") int BPF_PROG(test_1, struct bpf_dummy_struct_ops *ops, access state ...) Might be removed by verifier, thus triggering NULL pointer dereference under certain conditions.
CVE-2024-42152	In the Linux kernel, the following vulnerability has been resolved: nvmet: fix a possible leak when destroy a ctrl during destroy. We capture sq->ctrl early and if it is non-NULL we know that a ctrl was allocated (in the admin connect request handler). We clear ctrl->sqs and sq->ctrl (for nvme-loop primarily), and drop the final reference on the ctrl. However, a small window exists where sq->ctrl starts (as a result of the client giving up and disconnecting) concurrently with the nvme admin connect cmd (which kills and confirms of sq->ref (i.e. the admin connect managed to get an sq live reference). In this case, sq->ctrl was a local variable in nvmet_sq_destroy. This prevented the final reference drop on the ctrl. Solve this by re-capturing sq->ctrl after the admin connect completed, where for sure sq->ctrl reference is final, and move forward based on that. This issue was observed in a race condition where multiple ctrls simultaneously, creating a delay in allocating a ctrl leading up to this race window.
CVE-2024-42153	In the Linux kernel, the following vulnerability has been resolved: i2c: pnx: Fix potential deadlock warning from del_timer_sync() is called in an interrupt context it throws a warning because of potential deadlock. The timer is used to clear the timer after a timeout so replacing the call with wait_for_completion_timeout() allows to remove the problematic timer and avoid the warning.
CVE-2024-42154	In the Linux kernel, the following vulnerability has been resolved: tcp_metrics: validate source addr length I don't see any validation that TCP_METRICS_ATTR_SADDR_IPV4 is at least 4 bytes long, and the policy doesn't have an entry for this attribute (it should be manually validated).
CVE-2024-42155	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe copies of protected- and secure-keys. If protected- nor secure-keys is accessible, this key material should only be visible to the calling process. So wipe all key material from stack, even in case of an error.
CVE-2024-42156	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe copies of clear-key structures. For all IOCTLS, which convert a clear-key into a protected- or secure-key.
CVE-2024-42157	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe sensitive data on failure Wipe sensitive data on copy_to_user() fails.
CVE-2024-42158	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Use kfree_sensitive() to fix Coccinelle warnings and kfree() with kfree_sensitive() to fix warnings reported by Coccinelle: WARNING opportunity for kfree_sensitive/kvfree_sensitive (line 1643) WARNING opportunity for kfree_sensitive/kvfree_sensitive
CVE-2024-42159	In the Linux kernel, the following vulnerability has been resolved: scsi: mpi3mr: Sanitise num_phys Information is larger than size of this field shouldn't be allowed.
CVE-2024-42160	In the Linux kernel, the following vulnerability has been resolved: f2fs: check validation of fault attrs in f2fs_build_fault_attr in parse_options(), let's fix to add check condition in f2fs_build_fault_attr(). - Use f2fs_build_fault_attr()

CVE-2024-42161	In the Linux kernel, the following vulnerability has been resolved: bpf: Avoid uninitialized value in BPF_CORE_READ. Use a default branch in the switch statement to initialize 'val'.] GCC warns that 'val' may be used uninitialized in the function defined in bpf_core_read.h as: [...] unsigned long long val; \ [...] \ switch (__CORE_RELO(s, field, BYTE_SIZE)) { case 1: val = *(const unsigned short *)p; break; \ case 2: val = *(const unsigned short *)p; break; \ case 4: val = *(const unsigned int *)p; break; \ case 8: val = *(const unsigned long *)p; break; \ [...] val; \ } \ This patch adds a default entry in the switch statement that sets 'val' to zero in order to avoid the warning. __builtin_preserve_field_info returns unexpected values for BPF_FIELD_BYTE_SIZE. Tested in bpf-next master.
CVE-2024-42162	In the Linux kernel, the following vulnerability has been resolved: gve: Account for stopped queues when reading stats. A NIC might send us stats for a subset of queues. Without this change, gve_get_ethtool_stats might make an invalid assumption.
CVE-2024-42223	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: tda10048: Fix integer overflow. A multiplication can overflow a 32 bit integer when multiplied by pll_mfactor. Create a new 64 bit variable to hold the calculations.
CVE-2024-42224	In the Linux kernel, the following vulnerability has been resolved: net: dsa: mv88e6xxx: Correct check for empty list. mv88e6xxx: Support multiple MDIO busses") mv88e6xxx_default_mdio_bus() has checked that the return value of mv88e6xxx_mdio_read() is not zero to be intended to guard against the list chip->mdios being empty. However, it is not the correct check as the implementation can return NULL for empty lists. Instead, use list_first_entry_or_null() which does return NULL if the list is empty. Fix the check.
CVE-2024-42225	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: replace skb_put with skb_put_zero. A memset call is not needed as skb_put already zeroizes the memory.
CVE-2024-42226	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: prevent potential failure in handle_tx. Some transfer events don't always point to a TRB, and consequently don't have a endpoint ring. In these cases, function xhci_handle_tx_event() because if 'ep->skip' is set, the pointer to the endpoint ring is used. To prevent a potential failure and make the code more robust, add a code for a Transfer event without TRBs.
CVE-2024-42227	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix overlapping copy within copy engine. &mode_lib->mp.Watermark and &locals->Watermark are the same address. memcpy may lead to unexpected behavior.
CVE-2024-42228	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Using uninitialized value *size when calculating the size before calling amdgpu_vce_cs_reloc, such as case 0x03000001. V2: To really improve the handling we would need to use 0xffffffff.(Christian)
CVE-2024-42229	In the Linux kernel, the following vulnerability has been resolved: crypto: aead,cipher - zeroize key buffer after use. Variables temporarily holding cryptographic information should be zeroized once they are no longer needed. According to the buffers that previously held the private key.
CVE-2024-42230	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Fix scv instruction crash with relocation (reloc_on_exc), required for scv instruction support, before other CPUs have been shut down. This means they cannot be disabled, which causes an interrupt at an unexpected entry location that crashes the kernel. Change the kexec sequence to have been brought down. As a refresher, the real-mode scv interrupt vector is 0x17000, and the fixed-location head of the interrupt implementing such high addresses so it was just decided not to support that interrupt at all.
CVE-2024-4317	Missing authorization in PostgreSQL built-in views pg_stats_ext and pg_stats_ext_exprs allows an unprivileged database user to read and other statistics from CREATE STATISTICS commands of other users. The most common values may reveal confidential data, not otherwise read or results of functions they cannot execute. Installing an unaffected version only fixes fresh PostgreSQL installations are created with the initdb utility after installing that version. Current PostgreSQL installations will remain vulnerable until the release notes. Within major versions 14-16, minor versions before PostgreSQL 16.3, 15.7, and 14.12 are affected. All other versions are unaffected.
DSA-5349-1	gnutls28 - security update
DSA-5402-1	linux - security update
DSA-5453-1	linux - security update
DSA-5461-1	linux - security update
DSA-5475-1	linux - security update
DSA-5480-1	linux - security update
DSA-5523-1	curl - security update
DSA-5523-1	curl - security update
DSA-5570-1	nghttp2 - security update
DSA-5587-1	curl - security update
DSA-5587-1	curl - security update
DSA-5594-1	linux - security update
DSA-5681-1	linux - security update
DSA-5703-1	linux - security update

DSA-5730-1	linux - security update
GHSA-9h6g-pr28-7cqp	### Summary A ReDoS vulnerability occurs when nodemailer tries to parse img files with the parameter `attachData` event loop. Another flaw was found when nodemailer tries to parse an attachments with a embedded file, causing the event loop to stall. Regexp: /data:((?:[^\s;]* (?:"(?:[^\s"]*" \\\"))* '(?:[^\s']* \\')*))/ Path: compile -> getAttachments -> _processDataUrl Regexp: /(<img\b ^>[^\s"> > s +])/ Path: _convertDataImages ### PoC https://gist.github.com/francoatmega/890dd5053375333e40c6fdbcc9a9a042b0b24968d7b7039818e8b2698 ### Impact ReDoS causes the event loop to stuck a specially crafted image file.
RHSA-2022:4991	XZ Utils is an integrated collection of user-space file compression utilities based on the Lempel-Ziv-Markov chain algorithm. The algorithm provides a high compression ratio while keeping the decompression time short.
RHSA-2022:5056	The Common UNIX Printing System (CUPS) provides a portable printing layer for Linux, UNIX, and similar operating systems.
RHSA-2022:5311	The libgcrypt library provides general-purpose implementations of various cryptographic algorithms.
RHSA-2022:5313	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols.
RHSA-2022:5314	Expat is a C library for parsing XML documents.
RHSA-2022:5317	The libxml2 library is a development toolbox providing the implementation of various XML standards.
RHSA-2022:5696	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit.
RHSA-2022:5809	The pcre2 package contains a new generation of the Perl Compatible Regular Expression libraries for implementing regular expressions with the same syntax and semantics as Perl.
RHSA-2022:6159	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols.
RHSA-2022:6180	The rsync utility enables the users to copy and synchronize files locally or across a network. Synchronization with rsync is done by sending differences in files over the network instead of sending whole files. The rsync utility is also used as a mirroring tool.
RHSA-2022:6206	The systemd packages contain systemd, a system and service manager for Linux, compatible with the SysV and LSB init systems. It has parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemons, and supports Linux cgroups. In addition, it supports snapshotting and restoring of the system state, maintains mount and automount units, and transactional dependency-based service control logic. It can also work as a drop-in replacement for sysvinit.
RHSA-2022:6457	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems.
RHSA-2022:6463	The GNU Privacy Guard (GnuPG or GPG) is a tool for encrypting data and creating digital signatures, compliant with the OpenPGP standard.
RHSA-2022:6878	Expat is a C library for parsing XML documents.
RHSA-2022:7006	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit.
RHSA-2022:7089	KSBA (pronounced Kasbah) is a library to make X.509 certificates as well as the CMS easily accessible by other applications. It handles blocks of S/MIME and TLS.
RHSA-2022:7105	The gnutls packages provide the GNU Transport Layer Security (GnuTLS) library, which implements cryptographic protocols: TLS, DTLS, and DTLS.
RHSA-2022:7106	The zlib packages provide a general-purpose lossless data compression library that is used by many different programs.
RHSA-2022:7108	SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of a database without the administrative hassles of supporting a separate database server.
RHSA-2022:7704	WebKitGTK is the port of the portable web rendering engine WebKit to the GTK platform.
RHSA-2022:7715	The libxml2 library is a development toolbox providing the implementation of various XML standards.
RHSA-2022:7720	The e2fsprogs packages provide a number of utilities for creating, checking, modifying, and correcting the ext2, ext3, and ext4 file systems.
RHSA-2022:7745	FreeType is a free, high-quality, portable font engine that can open and manage font files. FreeType loads, hints, and renders fonts to various software renderers.
RHSA-2022:7793	The rsync utility enables the users to copy and synchronize files locally or across a network. Synchronization with rsync is done by sending differences in files over the network instead of sending whole files. The rsync utility is also used as a mirroring tool.
RHSA-2023:0110	SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of a database without the administrative hassles of supporting a separate database server.
RHSA-2023:0200	The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit.
RHSA-2023:0208	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit.
RHSA-2023:1095	The zlib packages provide a general-purpose lossless data compression library that is used by many different programs.

RHSA-2023:1140	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2023:1252	Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of securit
RHSA-2023:1332	Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of securit
RHSA-2023:1335	OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocol cryptography library.
RHSA-2023:1895	The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Sof
RHSA-2023:1908	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Sof
RHSA-2023:2963	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2023:2963	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2023:3106	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2023:3555	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exce and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing
RHSA-2023:4175	The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Sof
RHSA-2023:4176	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Sof
RHSA-2023:4864	The Common UNIX Printing System (CUPS) provides a portable printing layer for Linux, UNIX, and similar oper
RHSA-2023:5615	The libssh2 packages provide a library that implements the SSH2 protocol.
RHSA-2023:5731	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Sof
RHSA-2023:5742	The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Sof
RHSA-2023:5998	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exce and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing
RHSA-2023:6885	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exce and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing
RHSA-2023:7034	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exce and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing
RHSA-2023:7743	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2023:7783	PostgreSQL is an advanced object-relational database management system (DBMS).
RHSA-2024:0266	The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Sof
RHSA-2024:0533	The gnutls packages provide the GNU Transport Layer Security (GnuTLS) library, which implements cryptographic TLS, and DTLS.
RHSA-2024:0606	OpenSSH is an SSH protocol implementation supported by a number of Linux, UNIX, and similar operating system both the OpenSSH client and server.
RHSA-2024:0606	OpenSSH is an SSH protocol implementation supported by a number of Linux, UNIX, and similar operating system both the OpenSSH client and server.
RHSA-2024:0811	The sudo packages contain the sudo utility which allows system
RHSA-2024:0894	MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and
RHSA-2024:1129	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2024:1431	Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to per
RHSA-2024:1510	Node.js is a software development platform for building fast and scalable
RHSA-2024:1822	The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Sof
RHSA-2024:1879	The gnutls package provide the GNU Transport Layer Security (GnuTLS) library, which implements cryptographic and DTLS.
RHSA-2024:2463	The systemd packages contain systemd, a system and service manager for Linux, compatible with the SysV and LSB parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemon Linux cgroups. In addition, it supports snapshotting and restoring of the system state, maintains mount and automount transactional dependency-based service control logic. It can also work as a drop-in replacement for sysvinit.

RHSA-2024:2512	The file command is used to identify a particular file according to the type of data the file contains. It can identify n Executable and Linkable Format (ELF) binary files, system libraries, RPM packages, and different graphics format
RHSA-2024:2679	The libxml2 library is a development toolbox providing the implementation of various XML standards.
RHSA-2024:2780	Node.js is a software development platform for building fast and scalable network applications in the JavaScript pr
RHSA-2024:2987	Python is an interpreted, interactive, object-oriented programming language that supports modules, classes, excepti dynamic typing. The python27 packages provide a stable release of Python 2.7 with a number of additional utilities PostgreSQL.
RHSA-2024:2988	The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc
RHSA-2024:3254	The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc
RHSA-2024:3271	The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS s
RHSA-2024:3346	Git Large File Storage (LFS) replaces large files such as audio samples, videos, datasets, and graphics with text poi contents on a remote server.
RHSA-2024:3546	Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to per
RHSA-2024:3588	The glibc packages provide the standard C libraries (libc), POSIX thread
RHSA-2024:3834	The gdk-pixbuf2 packages provide an image loading library that can be extended
RHSA-2024:3968	The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc
SUSE-SU-2023:4659-1	Security update for curl
SUSE-SU-2023:4891-1	Security update for ncurses
SUSE-SU-2024:0070-1	Security update for tar
SUSE-SU-2024:0136-1	Security update for pam
SUSE-SU-2024:0140-1	Security update for libssh
SUSE-SU-2024:0305-1	Security update for cpio
SUSE-SU-2024:0549-1	Security update for openssl-1_1
SUSE-SU-2024:0555-1	Security update for libxml2
SUSE-SU-2024:0973-1	Security update for tiff
SUSE-SU-2024:0997-1	Security update for krb5
SUSE-SU-2024:1014-1	Security update for avahi
SUSE-SU-2024:1103-1	Security update for qemu
SUSE-SU-2024:1129-1	Security update for expat
SUSE-SU-2024:1133-1	Security update for ncurses
SUSE-SU-2024:1136-1	Security update for c-ares
SUSE-SU-2024:1151-1	Security update for curl
SUSE-SU-2024:1167-1	Security update for nghttp2
SUSE-SU-2024:1172-1	Security update for util-linux
SUSE-SU-2024:1271-1	Security update for gnutls
SUSE-SU-2024:1438-1	Security update for qemu
SUSE-SU-2024:1981-1	Security update for iperf
TEMP-0000000-F7A20F	Kernel: Unprivileged user can freeze journald

CDP Private Cloud Data Services 1.5.4-CHF3

The cumulative hotfixes for new features, known issues, and fixed issues for 1.5.4-CHF3.



Note: ECS Customers: Direct upgrade path is not available for customers currently on CDP Private Cloud Data Services 1.5.2. Customers must upgrade to CDP Private Cloud Data Services 1.5.4 prior to consuming any CHF3s built on top of 1.5.4.



Note:

OCP Customers: Direct upgrade path is available. Customers can directly upgrade from CDP Private Cloud Data Services 1.5.2 to any 1.5.4 CHF3s.

Whats new in CDP Private Cloud Data Services 1.5.4-CHF3

New features introduced in this cumulative hotfix release of CDP Private Cloud Data Services 1.5.4-CHF3.



Note: [Cloudera Manager 7.11.3 CHF9.1](#) (version: 7.11.3.24) supports CDP Private Cloud Data Services 1.5.4 CHF3 release.



Note: Cloudera Manager 7.11.3 CHF8 does not support any CDP Private Cloud Data Services release.



Note: Base 7.1.7 SP3, 7.1.9 CHF6, and 7.1.9 SP1 supports CDP Private Cloud Data Services 1.5.4 CHF3 release.



Note: CDP Private Cloud Data Services 1.5.4 CHF3 is certified with RHEL 8.10 and RHEL 9.4 (RHCK kernel only).

Known Issues in CDP Private Cloud Data Services 1.5.4-CHF3

New known issues in the 1.5.4 cumulative hotfix CHF3 release of CDP Private Cloud Data Services.

DOCS-22277 - CDP Private Cloud ECS longhorn upgrade failure

The helm-install-longhorn pod enters a crash loop state during ECS upgrade.

Provide the Longhorn diagnostic bundle to facilitate issue identification.



Note: Starting from 1.5.4 CHF3, Longhorn upgrade in ECS has a failure policy set to "abort" to prevent unexpected uninstallation triggers during retries.

Resuming Longhorn Upgrade: After resolving the underlying longhorn upgrade failure issues, follow these steps to resume the upgrade:

```
# Get the history of longhorn helm chart so that we can identify
the chart for which installation is failing. # helm history lon
ghorn -n longhorn-system
REVISION      UPDATED          STATUS      CHART
APP VERSION   DESCRIPTION
1             Thu Sep 26 21:31:05 2024    superseded  longhorn-1
.5.4          v1.5.4           Install complete
2             Fri Sep 27 05:17:44 2024    failed      longhorn-1
.6.2          v1.6.2           Upgrade "longhorn" failed: post-upgrade h
ooks failed: 1 error occurr...# Get the log of the failing helm-
install-longhorn job in the longhorn namespace
```

```
The job log should indicate that the due to failure policy being
"abort", it is waiting for manual intervention:
"Release status is 'failed' and failure policy is 'abort', not
'reinstall'; waiting for operator intervention"# We want to roll
back
```

```
# Find all jobs in longhorn-system and delete those. These jobs
will be re-triggered as part of the manual patch.
# kubectl get jobs -n longhorn-system
NAME                                COMPLETIONS  DURATION  AGE
```

```

helm-install-longhorn    0/1          9h          9h
longhorn-post-upgrade    1/1          11m         10h

# Delete all the longhorn jobs if any

# kubectl delete job helm-install-longhorn longhorn-post-upgrade
-n longhorn-system# Rollback longhorn to the version prior to the upgrade
# In this case, revision 1 marks the step of a successful longhorn 1.5.4 install
# helm rollback longhorn -n longhorn-system <revision number># Resume longhorn upgrade from Cloudera Manager UI
Running commands > All recent commands > find the failed upgrade command and click on resume

```

OPSX-5573/OPSAPS-69892 - Intermittent kube-proxy failures - 1.5.4 CHF3

After rebooting/restarting an ECS agent node, the kube-proxy Linux process may not start due to a race condition in the kubelet. When this happens, ECS cluster networking and other services – such as Vault, DNS, authentication, Longhorn storage, etc. – are affected. At the Kubernetes pod level, errors such as "connection refused", "connection timed out" and "i/o timeout" may be observed. If you suspect possible networking issues in your ECS cluster, checking kube-proxy is a good first step.

To fix this issue, perform the following steps on all of the affected nodes:

1. To identify which agent needs to be restarted, check the status of each kube-proxy pod to make sure it is in the "ready" state by running the following command on each host in the cluster.

```
kubectl describe pod [***POD-NAME***] -n kube-system
```

Here, [***POD-NAME***] should have a format such as: kube-proxy-<hostname>.

In the Conditions section of the describe pod output, confirm that the "ready" condition is "True".

```

Conditions:
  Type              Status
  Initialized        True
  Ready              True
  ContainersReady    True
  PodScheduled       True

```

Another option is to run the following command:

```

kubectl get pods -n kube-system -l component=kube-proxy -o go-template='{{range .items}}
{{.metadata.name}}{{"\n"}}{{"  "}}{{range .status.conditions}}
{{ if eq .type "Ready" }}
Ready:{{.status}}{{"\n\n"}}{{end}}{{end}}{{end}}'

```

The sample output displays the status of all of the kube-proxy pods in the cluster:

```

kube-proxy-host-1.cloudera.com
  Ready:True

kube-proxy-host-2.cloudera.com
  Ready:True

kube-proxy-host-3.cloudera.com
  Ready:True

```

- If the "ready" state is False, kube-proxy is not functioning properly, regardless of whether the kube-proxy process is running on that host or not. On each of the affected nodes, run the following command to delete the kube-proxy pod manifest:

```
rm /var/lib/rancher/rke2/agent/pod-manifests/kube-proxy.yaml
```

- Start the agent role.

After the agent role is started, you may not immediately see the kube-proxy process running, but a new kube-proxy process should start shortly. Check the pod status to make sure it is ready. After all of the problem agents have been restarted, the cluster may complain that the vault is sealed – if so, unseal it. At this point, the Control Plane should be functioning properly.

If current version is 1.5.2 perform above steps. If it is 1.5.3 or above, perform step 1 from the above procedure to identify the problematic nodes. Perform stop and start of ECS roles on the hosts where the problem exists.

Additional details about this issue are available here: <https://www.suse.com/support/kb/doc/?id=000021284>

COMPX-18031 - [ECS] [154CHF1-CHF3] Any new pods are stuck in pending state post ecs upgrade

When pods are stuck in pending state post ECS upgrade, you will not be able to schedule new workload (warehouse, virtual cluster etc) . Pending pods are normal if resources or quotas are exhausted. After high cluster loads, pods will be left in a pending state even if enough resources are available. The pods are not evaluated as part of normal scheduling.

The issue will be fixed after restarting the YuniKorn scheduler pod in yunikorn namespace. YuniKorn scheduler will trigger a re-evaluation of all pods and schedule the pending pods.

OBS-4176 - Prometheus reports duplicate metric alert for Kubernetes state metrics

After installing CDP Private Cloud Data Services 1.5.4, the EnvPrometheusDuplicateTimestamps warning message appears on the Control Plane Monitoring dashboard.

Perform the following steps:

- On the Management Console home page, select Administration > Alerts .
- On the Alerts page, search for the EnvPrometheusDuplicateTimestamps rule alert and from the drop-down menu select Disable Alert Rule to disable the alert.

Repository Locations for 1.5.4-CHF3

The URLs for CDP Private Cloud Data Services 1.5.4-CHF3 are listed in the following table:

URL Type	Repository Location
Index	<code>https://username:password@archive.cloudera.com/p/cdp-pvc-ds/1.5.4-h4/</code>
Manifest	Repository: <code>https://username:password@archive.cloudera.com/p/cdp-pvc-ds/1.5.4-h4/manifest.json</code>
Parcels	Repository: <code>https://username:password@archive.cloudera.com/p/cdp-pvc-ds/1.5.4-h4/parcels/</code>

Fixed Common Vulnerabilities and Exposures in 1.5.4 CHF3

Review the Common vulnerabilities and Exposures (CVEs) that were fixed in 1.5.4 CHF3 release of CDP Private Cloud Data Services.

Issue ID	Description
CVE-2013-0340	expat 2.1.0 and earlier does not properly handle entities expansion unless an application developer uses the XML_5 remote attackers to cause a denial of service (resource consumption), send HTTP requests to intranet servers, or read aka an XML External Entity (XXE) issue. NOTE: it could be argued that because expat already provides the ability responsibility for resolving this issue lies with application developers; according to this argument, this entry should would need its own CVE.
CVE-2014-9471	The parse_datetime function in GNU coreutils allows remote attackers to cause a denial of service (crash) or possibly string, as demonstrated by the "--date=TZ="123"345" @1" string to the touch or date command.
CVE-2015-4041	The keycompare_mb function in sort.c in sort in GNU Coreutils through 8.23 on 64-bit platforms performs a size c bytes occupied by multibyte characters, which allows attackers to cause a denial of service (heap-based buffer over unspecified other impact via long UTF-8 strings.
CVE-2015-4042	Integer overflow in the keycompare_mb function in sort.c in sort in GNU Coreutils through 8.23 might allow attack crash) or possibly have unspecified other impact via long strings.
CVE-2017-18018	In GNU Coreutils through 8.29, chown-core.c in chown and chgrp does not prevent replacement of a plain file with options, which allows local users to modify the ownership of arbitrary files by leveraging a race condition.
CVE-2018-13410	Info-ZIP Zip 3.0, when the -T and -TT command-line options are used, allows attackers to cause a denial of service possibly have unspecified other impact because of an off-by-one error. NOTE: it is unclear whether there are realistic controls the -TT value, given that the entire purpose of -TT is execution of arbitrary commands
CVE-2019-5068	An exploitable shared memory permissions vulnerability exists in the functionality of X11 Mesa 3D Graphics Library memory without any specific permissions to trigger this vulnerability.
CVE-2019-9704	Vixie Cron before the 3.0pl1-133 Debian package allows local users to cause a denial of service (daemon crash) via value is not checked.
CVE-2019-9705	Vixie Cron before the 3.0pl1-133 Debian package allows local users to cause a denial of service (memory consumption unlimited number of lines is accepted.
CVE-2020-25659	python-cryptography 3.2 is vulnerable to Bleichenbacher timing attacks in the RSA decryption API, via timed processing
CVE-2020-8201	Node.js < 12.18.4 and < 14.11 can be exploited to perform HTTP desync attacks and deliver malicious payloads to be crafted by an attacker to hijack user sessions, poison cookies, perform clickjacking, and a multitude of other attacks underlying system. The attack was possible due to a bug in processing of carrier-return symbols in the HTTP header
CVE-2021-20312	A flaw was found in ImageMagick in versions 7.0.11, where an integer overflow in WriteTHUMBNAIImage of o behavior via a crafted image file that is submitted by an attacker and processed by an application using ImageMagick is to system availability.
CVE-2021-20313	A flaw was found in ImageMagick in versions before 7.0.11. A potential cipher leak when the calculate signatures highest threat from this vulnerability is to data confidentiality.
CVE-2022-1125	Use after free in Portals in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user potentially exploit heap corruption via user interaction.
CVE-2022-1127	Use after free in QR Code Generator in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user interaction to potentially exploit heap corruption via user interaction.
CVE-2022-1131	Use after free in Cast UI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via user interaction.
CVE-2022-1133	Use after free in WebRTC Perf in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via user interaction.
CVE-2022-1134	Type confusion in V8 in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via user interaction.
CVE-2022-1135	Use after free in Shopping Cart in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via user interaction.
CVE-2022-1136	Use after free in Tab Strip in Google Chrome prior to 100.0.4896.60 allowed an attacker who convinced a user to interact to exploit heap corruption via specific set of user gestures.
CVE-2022-1137	Inappropriate implementation in Extensions in Google Chrome prior to 100.0.4896.60 allowed an attacker who convinced a user to leak potentially sensitive information via a crafted HTML page.
CVE-2022-1138	Inappropriate implementation in Web Cursor in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to obscure the contents of the Omnibox (URL bar) via a crafted HTML page.

CVE-2022-1139	Inappropriate implementation in Background Fetch API in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1141	Use after free in File Manager in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to interact with a crafted HTML page to potentially exploit heap corruption via specific user gesture.
CVE-2022-1142	Heap buffer overflow in WebUI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to interact with a crafted HTML page to potentially exploit heap corruption via specific input into DevTools.
CVE-2022-1143	Heap buffer overflow in WebUI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to interact with a crafted HTML page to potentially exploit heap corruption via specific input into DevTools.
CVE-2022-1144	Use after free in WebUI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to interact with a crafted HTML page to potentially exploit heap corruption via specific input into DevTools.
CVE-2022-1145	Use after free in Extensions in Google Chrome prior to 100.0.4896.60 allowed an attacker who convinced a user to interact with a crafted HTML page to potentially exploit heap corruption via specific user interaction and profile destruction.
CVE-2022-1146	Inappropriate implementation in Resource Timing in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1232	Type confusion in V8 in Google Chrome prior to 100.0.4896.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1305	Use after free in storage in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1306	Inappropriate implementation in compositing in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1308	Use after free in BFCache in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1309	Insufficient policy enforcement in developer tools in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1310	Use after free in regular expressions in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1312	Use after free in storage in Google Chrome prior to 100.0.4896.88 allowed an attacker who convinced a user to interact with a crafted HTML page to perform a sandbox escape via a crafted Chrome Extension.
CVE-2022-1313	Use after free in tab groups in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1314	Type confusion in V8 in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1364	Type confusion in V8 Turbofan in Google Chrome prior to 100.0.4896.127 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1477	Use after free in Vulkan in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1478	Use after free in SwiftShader in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1479	Use after free in ANGLE in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1482	Inappropriate implementation in WebGL in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1483	Heap buffer overflow in WebGPU in Google Chrome prior to 101.0.4951.41 allowed a remote attacker who had convinced a user to interact with a crafted HTML page to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1484	Heap buffer overflow in Web UI Settings in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1485	Use after free in File System API in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1486	Type confusion in V8 in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to obtain potentially sensitive information via a crafted HTML page.
CVE-2022-1487	Use after free in Ozone in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1488	Inappropriate implementation in Extensions API in Google Chrome prior to 101.0.4951.41 allowed an attacker who convinced a user to interact with a crafted HTML page to leak cross-origin data via a crafted Chrome Extension.
CVE-2022-1490	Use after free in Browser Switcher in Google Chrome prior to 101.0.4951.41 allowed a remote attacker who convinced a user to interact with a crafted HTML page to potentially exploit heap corruption via a crafted HTML page.

CVE-2022-1491	Use after free in Bookmarks in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit user interaction.
CVE-2022-1492	Insufficient data validation in Blink Editing in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to exploit crafted HTML page.
CVE-2022-1493	Use after free in Dev Tools in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit user interaction.
CVE-2022-1494	Insufficient data validation in Trusted Types in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to exploit crafted HTML page.
CVE-2022-1496	Use after free in File Manager in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit user interaction.
CVE-2022-1497	Inappropriate implementation in Input in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to spoof crafted HTML page.
CVE-2022-1498	Inappropriate implementation in HTML Parser in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to exploit crafted HTML page.
CVE-2022-1499	Inappropriate implementation in WebAuthentication in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to exploit crafted HTML page.
CVE-2022-1500	Insufficient data validation in Dev Tools in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to exploit crafted HTML page.
CVE-2022-1501	Inappropriate implementation in iframe in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to leak data.
CVE-2022-1638	Heap buffer overflow in V8 Internationalization in Google Chrome prior to 101.0.4951.64 allowed a remote attacker to exploit crafted HTML page.
CVE-2022-1639	Use after free in ANGLE in Google Chrome prior to 101.0.4951.64 allowed a remote attacker to potentially exploit user interaction.
CVE-2022-1640	Use after free in Sharing in Google Chrome prior to 101.0.4951.64 allowed a remote attacker who convinced a user to interact to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1853	Use after free in Indexed DB in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit user interaction.
CVE-2022-1854	Use after free in ANGLE in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit user interaction.
CVE-2022-1855	Use after free in Messaging in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit user interaction.
CVE-2022-1856	Use after free in User Education in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to interact to potentially exploit heap corruption via a crafted Chrome Extension or specific user interaction.
CVE-2022-1857	Insufficient policy enforcement in File System API in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to exploit crafted HTML page.
CVE-2022-1858	Out of bounds read in DevTools in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to perform an exploit via user interaction.
CVE-2022-1859	Use after free in Performance Manager in Google Chrome prior to 102.0.5005.61 allowed a remote attacker who convinced a user to interact to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1860	Use after free in UI Foundations in Google Chrome on Chrome OS prior to 102.0.5005.61 allowed a remote attacker who convinced a user to interact to potentially exploit heap corruption via specific user interactions.
CVE-2022-1861	Use after free in Sharing in Google Chrome on Chrome OS prior to 102.0.5005.61 allowed a remote attacker who convinced a user to interact to potentially exploit heap corruption via specific user interaction.
CVE-2022-1862	Inappropriate implementation in Extensions in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to interact to bypass profile restrictions via a crafted HTML page.
CVE-2022-1863	Use after free in Tab Groups in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to interact to exploit heap corruption via a crafted Chrome Extension and specific user interaction.
CVE-2022-1864	Use after free in WebApp Installs in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to interact to potentially exploit heap corruption via a crafted Chrome Extension and specific user interaction.
CVE-2022-1865	Use after free in Bookmarks in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to interact to exploit heap corruption via a crafted Chrome Extension and specific user interaction.
CVE-2022-1866	Use after free in Tablet Mode in Google Chrome on Chrome OS prior to 102.0.5005.61 allowed a remote attacker who convinced a user to interact to potentially exploit heap corruption via specific user interactions.

CVE-2022-1867	Insufficient validation of untrusted input in Data Transfer in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit heap corruption via a crafted clipboard content.
CVE-2022-1868	Inappropriate implementation in Extensions API in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to load an extension to bypass navigation restrictions via a crafted HTML page.
CVE-2022-1869	Type Confusion in V8 in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1870	Use after free in App Service in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to load an extension to exploit heap corruption via a crafted Chrome Extension.
CVE-2022-1871	Insufficient policy enforcement in File System API in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to load an extension to bypass file system policy via a crafted HTML page.
CVE-2022-1872	Insufficient policy enforcement in Extensions API in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to load an extension to bypass downloads policy via a crafted HTML page.
CVE-2022-1873	Insufficient policy enforcement in COOP in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1875	Inappropriate implementation in PDF in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to leak sensitive information via a crafted HTML page.
CVE-2022-1876	Heap buffer overflow in DevTools in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to load an extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1919	Use after free in Codecs in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2007	Use after free in WebGPU in Google Chrome prior to 102.0.5005.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2008	Double free in WebGL in Google Chrome prior to 102.0.5005.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2010	Out of bounds read in compositing in Google Chrome prior to 102.0.5005.115 allowed a remote attacker who had convinced a user to load an extension to potentially perform a sandbox escape via a crafted HTML page.
CVE-2022-2011	Use after free in ANGLE in Google Chrome prior to 102.0.5005.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2156	Use after free in Core in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2157	Use after free in Interest groups in Google Chrome prior to 103.0.5060.53 allowed a remote attacker who had convinced a user to load an extension to exploit heap corruption via a crafted HTML page.
CVE-2022-2158	Type confusion in V8 in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2161	Use after free in WebApp Provider in Google Chrome prior to 103.0.5060.53 allowed a remote attacker who convinced a user to load an extension to potentially exploit heap corruption via specific UI interactions.
CVE-2022-2163	Use after free in Cast UI and Toolbar in Google Chrome prior to 103.0.5060.134 allowed an attacker who convinced a user to load an extension to potentially exploit heap corruption via UI interaction.
CVE-2022-2164	Inappropriate implementation in Extensions API in Google Chrome prior to 103.0.5060.53 allowed an attacker who convinced a user to load an extension to bypass discretionary access control via a crafted HTML page.
CVE-2022-2165	Insufficient data validation in URL formatting in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to potentially exploit heap corruption via a crafted domain name.
CVE-2022-2294	Heap buffer overflow in WebRTC in Google Chrome prior to 103.0.5060.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2295	Type confusion in V8 in Google Chrome prior to 103.0.5060.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2399	Use after free in WebGPU in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2415	Heap buffer overflow in WebGL in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2477	Use after free in Guest View in Google Chrome prior to 103.0.5060.134 allowed an attacker who convinced a user to load an extension to exploit heap corruption via a crafted HTML page.
CVE-2022-2478	Use after free in PDF in Google Chrome prior to 103.0.5060.134 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2480	Use after free in Service Worker API in Google Chrome prior to 103.0.5060.134 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2481	Use after free in Views in Google Chrome prior to 103.0.5060.134 allowed a remote attacker who convinced a user to load an extension to potentially exploit heap corruption via UI interaction.
CVE-2022-2603	Use after free in Omnibox in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2022-2604	Use after free in Safe Browsing in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2605	Out of bounds read in Dawn in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2606	Use after free in Managed devices API in Google Chrome prior to 104.0.5112.79 allowed a remote attacker who convinced a user to interact with a page to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2610	Insufficient policy enforcement in Background Fetch in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2612	Side-channel information leakage in Keyboard input in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2022-2614	Use after free in Sign-In Flow in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2615	Insufficient policy enforcement in Cookies in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2616	Inappropriate implementation in Extensions API in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to interact with a page to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2022-2617	Use after free in Extensions API in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to interact with a page to potentially exploit heap corruption via specific UI interactions.
CVE-2022-2618	Insufficient validation of untrusted input in Internals in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a malicious file .
CVE-2022-2619	Insufficient validation of untrusted input in Settings in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to interact with a page to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2621	Use after free in Extensions in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to interact with a page to potentially exploit heap corruption via specific UI interactions.
CVE-2022-2624	Heap buffer overflow in PDF in Google Chrome prior to 104.0.5112.79 allowed a remote attacker who convinced a user to interact with a page to potentially exploit heap corruption via a crafted PDF file.
CVE-2022-2743	Integer overflow in Window Manager in Google Chrome on Chrome OS and Lacros prior to 104.0.5112.79 allowed a remote attacker who convinced a user to interact with a page to engage in specific UI interactions to perform an out of bounds memory write via crafted UI interactions. (Chrome OS only)
CVE-2022-2852	Use after free in FedCM in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2854	Use after free in SwiftShader in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2855	Use after free in ANGLE in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2857	Use after free in Blink in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2858	Use after free in Sign-In Flow in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page interaction.
CVE-2022-2859	Use after free in Chrome OS Shell in Google Chrome prior to 104.0.5112.101 allowed a remote attacker who convinced a user to interact with a page to potentially exploit heap corruption via specific UI interactions.
CVE-2022-2860	Insufficient policy enforcement in Cookies in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2861	Inappropriate implementation in Extensions API in Google Chrome prior to 104.0.5112.101 allowed an attacker who convinced a user to interact with a page to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2998	Use after free in Browser Creation in Google Chrome prior to 104.0.5112.101 allowed a remote attacker who had a user interact with a page to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-3038	Use after free in Network Service in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-3039	Use after free in WebSQL in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-3040	Use after free in Layout in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-3041	Use after free in WebSQL in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-3044	Inappropriate implementation in Site Isolation in Google Chrome prior to 105.0.5195.52 allowed a remote attacker who convinced a user to interact with a page to bypass site isolation via a crafted HTML page.

CVE-2022-3045	Insufficient validation of untrusted input in V8 in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to craft a crafted HTML page.
CVE-2022-3046	Use after free in Browser Tag in Google Chrome prior to 105.0.5195.52 allowed an attacker who convinced a user to visit a potentially exploit heap corruption via a crafted HTML page.
CVE-2022-3047	Insufficient policy enforcement in Extensions API in Google Chrome prior to 105.0.5195.52 allowed an attacker to convince a user to visit a potentially exploit heap corruption via a crafted HTML page.
CVE-2022-3054	Insufficient policy enforcement in DevTools in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to convince a user to visit a potentially exploit heap corruption via a crafted HTML page.
CVE-2022-3055	Use after free in Passwords in Google Chrome prior to 105.0.5195.52 allowed a remote attacker who convinced a user to visit a potentially exploit heap corruption via a crafted HTML page.
CVE-2022-3056	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to convince a user to visit a potentially exploit heap corruption via a crafted HTML page.
CVE-2022-3057	Inappropriate implementation in iframe Sandbox in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to convince a user to visit a potentially exploit heap corruption via a crafted HTML page.
CVE-2022-3058	Use after free in Sign-In Flow in Google Chrome prior to 105.0.5195.52 allowed a remote attacker who convinced a user to visit a potentially exploit heap corruption via crafted UI interaction.
CVE-2022-3075	Insufficient data validation in Mojo in Google Chrome prior to 105.0.5195.102 allowed a remote attacker who had access to a potentially perform a sandbox escape via a crafted HTML page.
CVE-2022-3195	Out of bounds write in Storage in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to perform an out of bounds write via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3196	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3197	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3198	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3199	Use after free in Frames in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3200	Heap buffer overflow in Internals in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3304	Use after free in CSS in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3307	Use after free in media in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3308	Insufficient policy enforcement in developer tools in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to convince a user to visit a potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-3311	Use after free in import in Google Chrome prior to 106.0.5249.62 allowed a remote attacker who had compromised a user to visit a potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-3312	Insufficient validation of untrusted input in VPN in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a remote attacker to convince a user to visit a potentially exploit heap corruption via physical access to the device. (Chromium security severity: Medium)
CVE-2022-3313	Incorrect security UI in full screen in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-3314	Use after free in logging in Google Chrome prior to 106.0.5249.62 allowed a remote attacker who had compromised a user to visit a potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-3315	Type confusion in Blink in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)
CVE-2022-3316	Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to convince a user to visit a potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)
CVE-2022-3370	Use after free in Custom Elements in Google Chrome prior to 106.0.5249.91 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

CVE-2022-3373	Out of bounds write in V8 in Google Chrome prior to 106.0.5249.91 allowed a remote attacker to perform an out of bounds write to memory. (Chromium security severity: High)
CVE-2022-3443	Insufficient data validation in File System API in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)
CVE-2022-3444	Insufficient data validation in File System API in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page and malicious file. (Chromium security severity: Low)
CVE-2022-3445	Use after free in Skia in Google Chrome prior to 106.0.5249.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3446	Heap buffer overflow in WebSQL in Google Chrome prior to 106.0.5249.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3448	Use after free in Permissions API in Google Chrome prior to 106.0.5249.119 allowed a remote attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3449	Use after free in Safe Browsing in Google Chrome prior to 106.0.5249.119 allowed an attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High)
CVE-2022-3450	Use after free in Peer Connection in Google Chrome prior to 106.0.5249.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3652	Type confusion in V8 in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3653	Heap buffer overflow in Vulkan in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3654	Use after free in Layout in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3655	Heap buffer overflow in Media Galleries in Google Chrome prior to 107.0.5304.62 allowed an attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-3656	Insufficient data validation in File System in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-3657	Use after free in Extensions in Google Chrome prior to 107.0.5304.62 allowed an attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: Medium)
CVE-2022-3661	Insufficient data validation in Extensions in Google Chrome prior to 107.0.5304.62 allowed a remote attacker who convinced a user to visit a malicious website to leak cross-origin data via a crafted Chrome extension. (Chromium security severity: Low)
CVE-2022-3723	Type confusion in V8 in Google Chrome prior to 107.0.5304.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3842	Use after free in Passwords in Google Chrome prior to 105.0.5195.125 allowed a remote attacker who had compromised a user's password to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3863	Use after free in Browser History in Google Chrome prior to 100.0.4896.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chrome security severity: High)
CVE-2022-3885	Use after free in V8 in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3886	Use after free in Speech Recognition in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3887	Use after free in Web Workers in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3888	Use after free in WebCodecs in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3889	Type confusion in V8 in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-3890	Heap buffer overflow in Crashpad in Google Chrome on Android prior to 107.0.5304.106 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4135	Heap buffer overflow in GPU in Google Chrome prior to 107.0.5304.121 allowed a remote attacker who had compromised a user's password to perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

CVE-2022-41724	Large handshake records may cause panics in crypto/tls. Both clients and servers may send large TLS handshake records, respectively, to panic when attempting to construct responses. This affects all TLS 1.3 clients, TLS 1.2 clients, and TLS 1.3 servers which request client certificates (by setting Config.ClientSessionCache to a non-nil value), and TLS 1.3 servers which request client certificates (RequestClientCert).
CVE-2022-41725	A denial of service is possible from excessive resource consumption in net/http and mime/multipart. Multipart form data parsing in multipart.Reader.ReadForm can consume largely unlimited amounts of memory and disk files. This also affects form parsing methods FormFile, FormValue, ParseMultipartForm, and PostFormValue. ReadForm takes a maxMemory parameter to limit memory consumption to maxMemory bytes + 10MB (reserved for non-file parts) in memory. File parts which cannot be stored in memory are written to disk. The unconfigurable 10MB reserved for non-file parts is excessively large and can potentially open a denial of service vulnerability. The limit of 10MB reserved for non-file parts is excessively large and can potentially open a denial of service vulnerability by not properly accounting for all memory consumed by a parsed form, such as map entry overhead, part names, and MIME headers. ReadForm can consume well over 10MB. In addition, ReadForm contained no limit on the number of disk files created, potentially creating a large number of disk temporary files. With fix, ReadForm now properly accounts for various forms of memory consumption and its documented limit of 10MB + maxMemory bytes of memory consumption. Users should still be aware that this limit is not strictly enforced. In addition, ReadForm now creates at most one on-disk temporary file, combining multiple form parts into a single file. The interface type's documentation states, "If stored on disk, the File's underlying concrete type will be an *os.File.". This is a change from more than one file part, due to this coalescing of parts into a single file. The previous behavior of using distinct files for each part is no longer supported. The environment variable GODEBUG=multipartfiles=distinct. Users should be aware that multipart.Reader.ReadForm and multipart.Writer.WriteForm limit the amount of disk consumed by temporary files. Callers can limit the size of form data with http.MaxBytesReader.
CVE-2022-4174	Type confusion in V8 in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4175	Use after free in Camera Capture in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4177	Use after free in Extensions in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced a user to install a Chrome Extension to exploit heap corruption via a crafted Chrome Extension and UI interaction. (Chromium security severity: High)
CVE-2022-4178	Use after free in Mojo in Google Chrome prior to 108.0.5359.71 allowed a remote attacker who had compromised a user's account to exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4179	Use after free in Audio in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced a user to install a Chrome Extension to exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High)
CVE-2022-4180	Use after free in Mojo in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced a user to install a Chrome Extension to exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High)
CVE-2022-4181	Use after free in Forms in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4182	Inappropriate implementation in Fenced Frames in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4183	Insufficient policy enforcement in Popup Blocker in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4184	Insufficient policy enforcement in Autofill in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4186	Insufficient validation of untrusted input in Downloads in Google Chrome prior to 108.0.5359.71 allowed an attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4189	Insufficient policy enforcement in DevTools in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced a user to install a Chrome Extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium)
CVE-2022-4190	Insufficient data validation in Directory in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4191	Use after free in Sign-In in Google Chrome prior to 108.0.5359.71 allowed a remote attacker who convinced a user to install a Chrome Extension to potentially exploit heap corruption via profile destruction. (Chromium security severity: Medium)
CVE-2022-4192	Use after free in Live Caption in Google Chrome prior to 108.0.5359.71 allowed a remote attacker who convinced a user to install a Chrome Extension to potentially exploit heap corruption via UI interaction. (Chromium security severity: Medium)
CVE-2022-4193	Insufficient policy enforcement in File System API in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4194	Use after free in Accessibility in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4195	Insufficient policy enforcement in Safe Browsing in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to exploit heap corruption via a malicious file. (Chromium security severity: Medium)

CVE-2022-4262	Type confusion in V8 in Google Chrome prior to 108.0.5359.94 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4436	Use after free in Blink Media in Google Chrome prior to 108.0.5359.124 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4437	Use after free in Mojo IPC in Google Chrome prior to 108.0.5359.124 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4438	Use after free in Blink Frames in Google Chrome prior to 108.0.5359.124 allowed a remote attacker who convinced the user to visit a malicious page to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4440	Use after free in Profiles in Google Chrome prior to 108.0.5359.124 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-46751	Improper Restriction of XML External Entity Reference, XML Injection (aka Blind XPath Injection) vulnerability in Apache Ivy. This issue affects any version of Apache Ivy prior to 2.5.2. When Apache Ivy prior to 2.5.2 parses XML files - Apache Maven POMs - it will allow downloading external document type definitions and expand any entity references used to exfiltrate data, access resources only the machine running Ivy has access to or disturb the execution of Ivy if DTD processing is disabled by default except when parsing Maven POMs where the default is to allow DTD processing with Ivy that is needed to deal with existing Maven POMs that are not valid XML files but are nevertheless accepted as valid XML files via newly introduced system properties where needed. Users of Ivy prior to version 2.5.2 can use Java system properties to disable DTDs, see the section about "JAXP Properties for External Access restrictions" inside Oracle's "Java API for XML Processing".
CVE-2022-4906	Inappropriate implementation in Blink in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to perform arbitrary read/write operations via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4907	Uninitialized Use in FFmpeg in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4908	Inappropriate implementation in iFrame Sandbox in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to perform arbitrary read/write operations via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4909	Inappropriate implementation in XML in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to perform arbitrary read/write operations via a crafted HTML page. (Chromium security severity: Low)
CVE-2022-4910	Inappropriate implementation in Autofill in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to perform arbitrary read/write operations via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4911	Insufficient data validation in DevTools in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Low)
CVE-2022-4912	Type Confusion in MathML in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4913	Inappropriate implementation in Extensions in Google Chrome prior to 105.0.5195.52 allowed a remote attacker who convinced the user to visit a malicious page to spoof extension storage via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4914	Heap buffer overflow in PrintPreview in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced the user to visit a malicious page to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4915	Inappropriate implementation in URL Formatting in Google Chrome prior to 103.0.5060.134 allowed a remote attacker to perform arbitrary read/write operations via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4916	Use after free in Media in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to perform arbitrary read/write operations via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4918	Use after free in UI in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to perform arbitrary read/write operations via a crafted HTML page. (Chromium security severity: Medium)
CVE-2022-4919	Use after free in Base Internals in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to perform arbitrary read/write operations via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4920	Heap buffer overflow in Blink in Google Chrome prior to 101.0.4951.41 allowed a remote attacker who convinced the user to visit a malicious page to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)
CVE-2022-4955	Inappropriate implementation in DevTools in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced the user to visit a malicious page to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-0129	Heap buffer overflow in Network Service in Google Chrome prior to 109.0.5414.74 allowed an attacker who convinced the user to visit a malicious page to potentially exploit heap corruption via a crafted HTML page and specific interactions. (Chromium security severity: High)
CVE-2023-0131	Inappropriate implementation in iFrame Sandbox in Google Chrome prior to 109.0.5414.74 allowed a remote attacker to perform arbitrary read/write operations via a crafted HTML page. (Chromium security severity: Medium)

CVE-2023-0134	Use after free in Cart in Google Chrome prior to 109.0.5414.74 allowed an attacker who convinced a user to install a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-0135	Use after free in Cart in Google Chrome prior to 109.0.5414.74 allowed an attacker who convinced a user to install a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-0138	Heap buffer overflow in libphonenumber in Google Chrome prior to 109.0.5414.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-0141	Insufficient policy enforcement in CORS in Google Chrome prior to 109.0.5414.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-0471	Use after free in WebTransport in Google Chrome prior to 109.0.5414.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-0472	Use after free in WebRTC in Google Chrome prior to 109.0.5414.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-0473	Type Confusion in ServiceWorker API in Google Chrome prior to 109.0.5414.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-0474	Use after free in GuestView in Google Chrome prior to 109.0.5414.119 allowed an attacker who convinced a user to install a Chrome web app to exploit heap corruption via a Chrome web app. (Chromium security severity: Medium)
CVE-2023-0696	Type confusion in V8 in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-0698	Out of bounds read in WebRTC in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to perform an out of bounds read via a crafted HTML page. (Chromium security severity: High)
CVE-2023-0699	Use after free in GPU in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-0700	Inappropriate implementation in Download in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-0701	Heap buffer overflow in WebUI in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who convinced a user to install a Chrome web app to potentially exploit heap corruption via UI interaction . (Chromium security severity: Medium)
CVE-2023-0702	Type confusion in Data Transfer in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who convinced a user to install a Chrome web app to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-0703	Type confusion in DevTools in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who convinced a user to install a Chrome web app to potentially exploit heap corruption via UI interactions. (Chromium security severity: Medium)
CVE-2023-0704	Insufficient policy enforcement in DevTools in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-0705	Integer overflow in Core in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who had one a race condition to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-0928	Use after free in SwiftShader in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-0929	Use after free in Vulkan in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-0930	Heap buffer overflow in Video in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-0931	Use after free in Video in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-0933	Integer overflow in PDF in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-0941	Use after free in Prompts in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)
CVE-2023-1213	Use after free in Swiftshader in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-1214	Type confusion in V8 in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

CVE-2023-1215	Type confusion in CSS in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit h (Chromium security severity: High)
CVE-2023-1216	Use after free in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had convience to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-1218	Use after free in WebRTC in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially explo (Chromium security severity: High)
CVE-2023-1219	Heap buffer overflow in Metrics in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had com exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-1220	Heap buffer overflow in UMA in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had comp exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-1221	Insufficient policy enforcement in Extensions API in Google Chrome prior to 111.0.5563.64 allowed an attacker w extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium)
CVE-2023-1222	Heap buffer overflow in Web Audio API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to po HTML page. (Chromium security severity: Medium)
CVE-2023-1224	Insufficient policy enforcement in Web Payments API in Google Chrome prior to 111.0.5563.64 allowed a remote a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-1226	Insufficient policy enforcement in Web Payments API in Google Chrome prior to 111.0.5563.64 allowed a remote a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-1229	Inappropriate implementation in Permission prompts in Google Chrome prior to 111.0.5563.64 allowed a remote a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-1232	Insufficient policy enforcement in Resource Timing in Google Chrome prior to 111.0.5563.64 allowed a remote att information from API via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-1233	Insufficient policy enforcement in Resource Timing in Google Chrome prior to 111.0.5563.64 allowed an attacker extension to obtain potentially sensitive information from API via a crafted Chrome Extension. (Chromium security severity: Low)
CVE-2023-1235	Type confusion in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compro exploit heap corruption via a crafted UI interaction. (Chromium security severity: Low)
CVE-2023-1236	Inappropriate implementation in Internals in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to sp HTML page. (Chromium security severity: Low)
CVE-2023-1528	Use after free in Passwords in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compro exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-1529	Out of bounds memory access in WebHID in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to malicious HID device. (Chromium security severity: High)
CVE-2023-1530	Use after free in PDF in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit h (Chromium security severity: High)
CVE-2023-1531	Use after free in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially explo (Chromium security severity: High)
CVE-2023-1532	Out of bounds read in GPU Video in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentia HTML page. (Chromium security severity: High)
CVE-2023-1533	Use after free in WebProtect in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially ex page. (Chromium security severity: High)
CVE-2023-1534	Out of bounds read in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had com exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-1810	Heap buffer overflow in Visuals in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who had com exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-1811	Use after free in Frames in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-1812	Out of bounds memory access in DOM Bindings in Google Chrome prior to 112.0.5615.49 allowed a remote attack via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-1813	Inappropriate implementation in Extensions in Google Chrome prior to 112.0.5615.49 allowed an attacker who cor to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium)

CVE-2023-1814	Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-1815	Use after free in Networking APIs in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-1816	Incorrect security UI in Picture In Picture in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-1817	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 112.0.5615.49 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-1818	Use after free in Vulkan in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-1819	Out of bounds read in Accessibility in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform a denial of service attack via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-1820	Heap buffer overflow in Browser History in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-1821	Inappropriate implementation in WebShare in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (URL bar) via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-1822	Incorrect security UI in Navigation in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform a denial of service attack via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-1823	Inappropriate implementation in FedCM in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass security checks via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-2033	Type confusion in V8 in Google Chrome prior to 112.0.5615.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-20883	In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2.5.14 and older unsupported versions, there is a denial of service attack if Spring MVC is used together with a reverse proxy cache.
CVE-2023-2133	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-2134	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-2135	Use after free in DevTools in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-2136	Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who had compromised a user's system to potentially exploit a sandbox escape via a crafted HTML page. (Chromium security severity: High)
CVE-2023-2137	Heap buffer overflow in sqlite in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-2311	Insufficient policy enforcement in File System API in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-2314	Insufficient data validation in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass security checks via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-23931	cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. In affected versions, the package would accept Python objects which implement the buffer protocol, but provide only immutable buffers. This would allow an attacker to mutate the buffers, thus violating fundamental rules of Python and resulting in corrupted output. This now correctly raises an exception. The fix, `update_into` was originally introduced in cryptography 1.8.
CVE-2023-24534	HTTP and MIME header parsing can allocate large amounts of memory, even when parsing small inputs, potentially leading to memory exhaustion and a denial of service. Unusual patterns of input data can cause the common function used to parse HTTP and MIME headers to allocate space to hold the parsed headers. An attacker can exploit this behavior to cause an HTTP server to allocate large amounts of memory, leading to memory exhaustion and a denial of service. With fix, header parsing now correctly allocates only the memory needed for the headers.

CVE-2023-24536	Multipart form parsing can consume large amounts of CPU and memory when processing form inputs containing v several causes: 1. mime/multipart.Reader.ReadForm limits the total memory a parsed multipart form can consume. memory consumed, leading it to accept larger inputs than intended. 2. Limiting total memory does not account for from large numbers of small allocations in forms with many parts. 3. ReadForm can allocate a large number of sho on the garbage collector. The combination of these factors can permit an attacker to cause an program that parses m of CPU and memory, potentially resulting in a denial of service. This affects programs that use mime/multipart.Re the net/http package with the Request methods FormFile, FormValue, ParseMultipartForm, and PostFormValue. W estimating the memory consumption of parsed forms, and performs many fewer short-lived allocations. In addition the following limits on the size of parsed forms: 1. Forms parsed with ReadForm may contain no more than 1000 p environment variable GODEBUG=multipartmaxparts=. 2. Form parts parsed with NextPart and NextRawPart may addition, forms parsed with ReadForm may contain no more than 10,000 header fields across all parts. This limit m GODEBUG=multipartmaxheaders=.
CVE-2023-2459	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to by HTML page. (Chromium security severity: Medium)
CVE-2023-2460	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed an attack extension to bypass file access checks via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-2462	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to ob page. (Chromium security severity: Medium)
CVE-2023-2464	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed an attacker wh extension to perform an origin spoof in the security UI via a crafted HTML page. (Chromium security severity: Me
CVE-2023-2465	Inappropriate implementation in CORS in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to leak (Chromium security severity: Medium)
CVE-2023-2466	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to sp crafted HTML page. (Chromium security severity: Low)
CVE-2023-2468	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed a remote attac process to obfuscate the security UI via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-26112	All versions of the package configobj are vulnerable to Regular Expression Denial of Service (ReDoS) via the valid This is only exploitable in the case of a developer, putting the offending value in a server side configuration file.
CVE-2023-2721	Use after free in Navigation in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exp page. (Chromium security severity: Critical)
CVE-2023-2723	Use after free in DevTools in Google Chrome prior to 113.0.5672.126 allowed a remote attacker who had comprom exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-2724	Type confusion in V8 in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit h (Chromium security severity: High)
CVE-2023-2725	Use after free in Guest View in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-2726	Inappropriate implementation in WebApp Installs in Google Chrome prior to 113.0.5672.126 allowed an attacker v web app to bypass install dialog via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-2929	Out of bounds write in Swiftshader in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentia HTML page. (Chromium security severity: High)
CVE-2023-2930	Use after free in Extensions in Google Chrome prior to 114.0.5735.90 allowed an attacker who convinced a user to exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-2931	Use after free in PDF in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit hea (Chromium security severity: High)
CVE-2023-2932	Use after free in PDF in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit hea (Chromium security severity: High)
CVE-2023-2933	Use after free in PDF in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit hea (Chromium security severity: High)
CVE-2023-2934	Out of bounds memory access in Mojo in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to pote HTML page. (Chromium security severity: High)
CVE-2023-2935	Type Confusion in V8 in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit he (Chromium security severity: High)
CVE-2023-2936	Type Confusion in V8 in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit he (Chromium security severity: High)

CVE-2023-2937	Inappropriate implementation in Picture In Picture in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-2938	Inappropriate implementation in Picture In Picture in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-2940	Inappropriate implementation in Downloads in Google Chrome prior to 114.0.5735.90 allowed an attacker who controls a web page to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-29406	The HTTP/1 client does not fully validate the contents of the Host header. A maliciously crafted Host header can in some cases cause a client to send requests to an unintended host. With fix, the HTTP/1 client now refuses to send requests containing an invalid Request.Host or Request.URL.Host header.
CVE-2023-2941	Inappropriate implementation in Extensions API in Google Chrome prior to 114.0.5735.90 allowed an attacker who controls a web page to spoof the contents of the UI via a crafted Chrome Extension. (Chromium security severity: Low)
CVE-2023-30581	The use of <code>__proto__</code> in <code>process.mainModule.__proto__.require()</code> can bypass the policy mechanism and require modules that are not allowed. This vulnerability affects all users using the experimental policy mechanism in all active release lines: v16, v18 and v20. As of Node.js v20.2.0, with fix, the policy is an experimental feature of Node.js
CVE-2023-30588	When an invalid public key is used to create an x509 certificate using the <code>crypto.X509Certificate()</code> API a non-exploitable vulnerability was discovered that could lead to DoS attacks when the attacker could force interruptions of application processing, as the process terminates when a certificate is created. The current context of the users will be gone, and that will cause a DoS scenario. This vulnerability was fixed in versions v16, v18, and, v20.
CVE-2023-30589	The <code>llhttp</code> parser in the <code>http</code> module in Node v20.2.0 does not strictly use the CRLF sequence to delimit HTTP request headers (HRS). The CR character (without LF) is sufficient to delimit HTTP header fields in the <code>llhttp</code> parser. A CRLF sequence should delimit each header-field. This impacts all Node.js active versions: v16, v18, and, v20
CVE-2023-30590	The <code>generateKeys()</code> API function returned from <code>crypto.createDiffieHellman()</code> only generates missing (or outdated) public and private keys if none has been set yet, but the function is also needed to compute the corresponding public key after calling <code>setPrivateKey()</code> . This API call: "Generates private and public Diffie-Hellman key values". The documented behavior is very different from what is actually happening. This could easily lead to security issues in applications that use these APIs as the DiffieHellman may be used as the basis for key exchange and are consequently broad.
CVE-2023-3079	Type confusion in V8 in Google Chrome prior to 114.0.5735.110 allowed a remote attacker to potentially exploit heap memory. (Chromium security severity: High)
CVE-2023-30861	Flask is a lightweight WSGI web application framework. When all of the following conditions are met, a response from the application may be cached and subsequently sent by the proxy to other clients. If the proxy also caches 'Set-Cookie' headers, the proxy may cache the 'session' cookie to other clients. The severity depends on the application's use of the session and the proxy's behavior. The conditions are: 1. The application must be hosted behind a caching proxy that does not purge cached responses. 2. The application sets 'session.permanent = True'. 3. The application does not access or modify the session object. 4. The application sets 'SESSION_REFRESH_EACH_REQUEST' enabled (the default). 5. The application does not set a 'Cache-Control' header. This happens because vulnerable versions of Flask only set the 'Vary: Cookie' header when the session is refreshed (re-sent to update the expiration) without being accessed or modified. This issue has been fixed in version 2.0.2.
CVE-2023-3214	Use after free in Autofill payments in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit heap memory via a crafted HTML page. (Chromium security severity: Critical)
CVE-2023-3215	Use after free in WebRTC in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit heap memory. (Chromium security severity: High)
CVE-2023-3216	Type confusion in V8 in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit heap memory. (Chromium security severity: High)
CVE-2023-3217	Use after free in WebXR in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit heap memory. (Chromium security severity: High)
CVE-2023-33953	gRPC contains a vulnerability that allows hpack table accounting errors could lead to unwanted disconnects between clients and servers. Three vectors were found that allow the following DOS attacks: - Unbounded memory buffering in the HPACK parser The unbounded CPU consumption is down to a copy that occurred per-input-block in the parser. Due to the memory copy bug we end up with an O(n^2) parsing loop, with n selected by the client. The unbounded memory consumption check was behind the string reading code, so we needed to first buffer up to a 4 gigabyte string before rejecting it and then rejecting it. - gRPC's metadata overflow check was performed per frame, so that the following sequence of requests could be sent: HEADERS: containing a: 1 CONTINUATION: containing a: 2 CONTINUATION: containing a: 3 etc, etc, etc
CVE-2023-34054	In Reactor Netty HTTP Server, versions 1.1.x prior to 1.1.13 and versions 1.0.x prior to 1.0.39, it is possible for a user to craft a request that may cause a denial-of-service (DoS) condition. Specifically, an application is vulnerable if Reactor Netty's Micrometer is enabled.
CVE-2023-34055	In Spring Boot versions 2.7.0 - 2.7.17, 3.0.0-3.0.12 and 3.1.0-3.1.5, it is possible for a user to provide specially crafted requests that may cause a denial-of-service (DoS) condition. Specifically, an application is vulnerable when all of the following are true: * the application is using Spring Boot's <code>org.springframework.boot:spring-boot-actuator</code> is on the classpath

CVE-2023-34062	In Reactor Netty HTTP Server, versions 1.1.x prior to 1.1.13 and versions 1.0.x prior to 1.0.39, a malicious user can craft a URL that can lead to a directory traversal attack. Specifically, an application is vulnerable if Reactor Netty HTTP Server is used.
CVE-2023-34110	Flask-AppBuilder is an application development framework, built on top of Flask. Prior to version 4.3.2, an authentication bypass, could by adding a special character on the add, edit User forms trigger a database error, this error is surfaced to the user. In some database engines this error can include the entire user row including the pbkdf2:sha256 hashed password. This vulnerability can be exploited to retrieve the password of any user.
CVE-2023-3420	Type Confusion in V8 in Google Chrome prior to 114.0.5735.198 allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-3421	Use after free in Media in Google Chrome prior to 114.0.5735.198 allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-3422	Use after free in Guest View in Google Chrome prior to 114.0.5735.198 allowed an attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-3598	Out of bounds read and write in ANGLE in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-3727	Use after free in WebRTC in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-37276	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. aiohttp v3.8.4 and earlier are built on top of the aiohttp library. The aiohttp library is used by aiohttp for its HTTP request parser when available which is the default case when installing from a package manager. If you are using aiohttp as an HTTP server (ie `aiohttp.Application`), you are not affected by this vulnerability if you are using aiohttp v3.8.5 or later. (ie `aiohttp.ClientSession`). Sending a crafted HTTP request will cause the server to misinterpret one of the HTTP request smuggling. This issue has been addressed in version 3.8.5. Users are advised to upgrade. Users unable to upgrade should set the environment variable `AIOHTTP_NO_EXTENSIONS=1` as an environment variable to disable the llhttp HTTP request parser implementation. (Chromium security severity: High)
CVE-2023-3728	Use after free in WebRTC in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-3730	Use after free in Tab Groups in Google Chrome prior to 115.0.5790.98 allowed a remote attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-3732	Out of bounds memory access in Mojo in Google Chrome prior to 115.0.5790.98 allowed a remote attacker who had access to a malicious website to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-3733	Inappropriate implementation in WebApp Installs in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-3734	Inappropriate implementation in Picture In Picture in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-3735	Inappropriate implementation in Web API Permission Prompts in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-3737	Inappropriate implementation in Notifications in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-3738	Inappropriate implementation in Autofill in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-3740	Insufficient validation of untrusted input in Themes in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit memory corruption via a user via a crafted background URL. (Chromium security severity: Low)
CVE-2023-37415	Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow Apache Hive Provider. Prior to version 6.1.2, the proxy_user option can also inject semicolon. This issue affects Apache Airflow Apache Hive Provider. Users are advised to update provider version to 6.1.2 in order to avoid this vulnerability.
CVE-2023-39321	Processing an incomplete post-handshake message for a QUIC connection can cause a panic.
CVE-2023-39322	QUIC connections do not set an upper bound on the amount of data buffered when reading post-handshake messages. This can cause unbounded memory growth. With fix, connections now consistently reject messages larger than 65KiB in size.
CVE-2023-4068	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to perform arbitrary read and write operations via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4069	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4070	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to perform arbitrary read and write operations via a crafted HTML page. (Chromium security severity: High)

CVE-2023-4071	Heap buffer overflow in Visuals in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4072	Out of bounds read and write in WebGL in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4074	Use after free in Blink Task Scheduling in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4075	Use after free in Cast in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4076	Use after free in WebRTC in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4077	Insufficient data validation in Extensions in Google Chrome prior to 115.0.5790.170 allowed an attacker who convinced a user to install a Chrome Extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: Medium)
CVE-2023-4078	Inappropriate implementation in Extensions in Google Chrome prior to 115.0.5790.170 allowed an attacker who convinced a user to install a Chrome Extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: Medium)
CVE-2023-41419	An issue in Gevent before version 23.9.0 allows a remote attacker to escalate privileges via a crafted script to the WebUI process. (Chromium security severity: High)
CVE-2023-4349	Use after free in Device Trust Connectors in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4351	Use after free in Network in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who has elicited a browser crash to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4352	Type confusion in V8 in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4353	Heap buffer overflow in ANGLE in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4354	Heap buffer overflow in Skia in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who had convinced a user to install a Chrome Extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4355	Out of bounds memory access in V8 in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4356	Use after free in Audio in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who has convinced a user to install a Chrome Extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-4357	Insufficient validation of untrusted input in XML in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-4358	Use after free in DNS in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-4360	Inappropriate implementation in Color in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to obfuscate a page. (Chromium security severity: Medium)
CVE-2023-4362	Heap buffer overflow in Mojom IDL in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who had convinced a user to install a Chrome Extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4364	Inappropriate implementation in Permission Prompts in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to obfuscate a page. (Chromium security severity: Medium)
CVE-2023-4365	Inappropriate implementation in Fullscreen in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to obfuscate a page. (Chromium security severity: Medium)
CVE-2023-4366	Use after free in Extensions in Google Chrome prior to 116.0.5845.96 allowed an attacker who convinced a user to install a Chrome Extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-4367	Insufficient policy enforcement in Extensions API in Google Chrome prior to 116.0.5845.96 allowed an attacker who convinced a user to install a Chrome Extension to bypass an enterprise policy via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-4368	Insufficient policy enforcement in Extensions API in Google Chrome prior to 116.0.5845.96 allowed an attacker who convinced a user to install a Chrome Extension to bypass an enterprise policy via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-4427	Out of bounds memory access in V8 in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-4428	Out of bounds memory access in CSS in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

CVE-2023-4429	Use after free in Loader in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: High)
CVE-2023-4430	Use after free in Vulkan in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: High)
CVE-2023-4431	Out of bounds memory access in Fonts in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: Medium)
CVE-2023-4572	Use after free in MediaStream in Google Chrome prior to 116.0.5845.140 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: High)
CVE-2023-47248	Deserialization of untrusted data in IPC and Parquet readers in PyArrow versions 0.14.0 to 14.0.0 allows arbitrary code execution if it reads Arrow IPC, Feather or Parquet data from untrusted sources (for example user-supplied input files). This affects other Apache Arrow implementations or bindings. It is recommended that users of PyArrow upgrade to 14.0.1. Similar libraries upgrade their dependency requirements to PyArrow 14.0.1 or later. PyPI packages are already available, and will be available soon. If it is not possible to upgrade, we provide a separate package `pyarrow-hotfix` that disables the vulnerable code. See https://pypi.org/project/pyarrow-hotfix/ for instructions.
CVE-2023-4761	Out of bounds memory access in FedCM in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: High)
CVE-2023-4762	Type Confusion in V8 in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to execute arbitrary code. (Chromium security severity: High)
CVE-2023-47627	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. The HTTP parser in AIOHTTP is vulnerable to request smuggling. This parser is only used when AIOHTTP_NO_EXTENSIONS is enabled (which has been addressed in commit `d5c12ba89` which has been included in release version 3.8.6. Users are advised to upgrade for these issues.
CVE-2023-4763	Use after free in Networks in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: High)
CVE-2023-4764	Incorrect security UI in BFCache in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to spoof the security UI. (Chromium security severity: High)
CVE-2023-4901	Inappropriate implementation in Prompts in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: Medium)
CVE-2023-4902	Inappropriate implementation in Input in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: Medium)
CVE-2023-4904	Insufficient policy enforcement in Downloads in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: Medium)
CVE-2023-4905	Inappropriate implementation in Prompts in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: Medium)
CVE-2023-4906	Insufficient policy enforcement in Autofill in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: Low)
CVE-2023-4908	Inappropriate implementation in Picture in Picture in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: Low)
CVE-2023-49081	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Improper validation made it possible for an attacker to control the HTTP version of the request (e.g. to insert a new header) or create a new HTTP request if the attacker controls the HTTP version. The vulnerability was patched in version 3.9.0.
CVE-2023-49082	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Improper validation makes it possible for an attacker to control the HTTP method (GET, POST etc.) of the request. If the attacker can control the HTTP version of the request (request smuggling). This issue has been patched in version 3.9.0.
CVE-2023-4909	Inappropriate implementation in Interstitials in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to potentially exploit a vulnerability. (Chromium security severity: Low)
CVE-2023-50658	The jose2go component before 1.6.0 for Go allows attackers to cause a denial of service (CPU consumption) via a crafted request.
CVE-2023-51764	Postfix through 3.8.5 allows SMTP smuggling unless configured with smtpd_data_restrictions=reject_unauth_pipelining or smtpd_discard_ehlo_keywords=chunking (or certain other options that exist in recent versions). Remote attackers can use this to inject e-mail messages with a spoofed MAIL FROM address, allowing bypass of an SPF protection mechanism. This issue has been patched in version 3.8.6, but some other popular e-mail servers do not. To prevent attack variants (by always disallowing the use of the <LF> character in the body of the message), the smtpd_forbid_bare_newline=yes option with a Postfix minimum version of 3.5.23, 3.6.13, 3.7.4 or later is required.

CVE-2023-5186	Use after free in Passwords in Google Chrome prior to 117.0.5938.132 allowed a remote attacker who convinced a user to enter a password to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: High)
CVE-2023-5187	Use after free in Extensions in Google Chrome prior to 117.0.5938.132 allowed an attacker who convinced a user to enter a password to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-5218	Use after free in Site Isolation in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)
CVE-2023-5346	Type confusion in V8 in Google Chrome prior to 117.0.5938.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-5472	Use after free in Profiles in Google Chrome prior to 118.0.5993.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-5473	Use after free in Cast in Google Chrome prior to 118.0.5993.70 allowed a remote attacker who had compromised the user's system to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-5474	Heap buffer overflow in PDF in Google Chrome prior to 118.0.5993.70 allowed a remote attacker who convinced a user to open a PDF file to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium)
CVE-2023-5475	Inappropriate implementation in DevTools in Google Chrome prior to 118.0.5993.70 allowed an attacker who convinced a user to install a Chrome Extension to bypass discretionary access control via a crafted Chrome Extension. (Chromium security severity: Medium)
CVE-2023-5476	Use after free in Blink History in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-5477	Inappropriate implementation in Installer in Google Chrome prior to 118.0.5993.70 allowed a local attacker to bypass discretionary access control via a crafted command. (Chromium security severity: Low)
CVE-2023-5478	Inappropriate implementation in Autofill in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to leak sensitive information via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-5479	Inappropriate implementation in Extensions API in Google Chrome prior to 118.0.5993.70 allowed an attacker who convinced a user to install a Chrome Extension to bypass an enterprise policy via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-5480	Inappropriate implementation in Payments in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-5481	Inappropriate implementation in Downloads in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-5482	Insufficient data validation in USB in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform a denial of service via a crafted HTML page. (Chromium security severity: High)
CVE-2023-5483	Inappropriate implementation in Intents in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-5484	Inappropriate implementation in Navigation in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-5485	Inappropriate implementation in Autofill in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-5486	Inappropriate implementation in Input in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to spoof input via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-5487	Inappropriate implementation in Fullscreen in Google Chrome prior to 118.0.5993.70 allowed an attacker who convinced a user to enter a password to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium)
CVE-2023-5849	Integer overflow in USB in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-5850	Incorrect security UI in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform a denial of service via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-5851	Inappropriate implementation in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-5852	Use after free in Printing in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to print a document to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium)
CVE-2023-5853	Incorrect security UI in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to obfuscate sensitive information via a crafted HTML page. (Chromium security severity: Medium)

CVE-2023-5854	Use after free in Profiles in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to interact with a malicious file to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium)
CVE-2023-5855	Use after free in Reading Mode in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to interact with a malicious file to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium)
CVE-2023-5856	Use after free in Side Panel in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to interact with a malicious file to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-5857	Inappropriate implementation in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially exploit heap corruption via a malicious file. (Chromium security severity: Medium)
CVE-2023-5858	Inappropriate implementation in WebApp Provider in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-5859	Incorrect security UI in Picture In Picture in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-5996	Use after free in WebAudio in Google Chrome prior to 119.0.6045.123 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-5997	Use after free in Garbage Collection in Google Chrome prior to 119.0.6045.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6112	Use after free in Navigation in Google Chrome prior to 119.0.6045.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6345	Integer overflow in Skia in Google Chrome prior to 119.0.6045.199 allowed a remote attacker who had compromised a sandbox escape via a malicious file. (Chromium security severity: High)
CVE-2023-6346	Use after free in WebAudio in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6347	Use after free in Mojo in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6348	Type Confusion in Spellcheck in Google Chrome prior to 119.0.6045.199 allowed a remote attacker who had compromised a sandbox escape via a malicious file to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6350	Use after free in libavif in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6351	Use after free in libavif in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6508	Use after free in Media Stream in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6509	Use after free in Side Panel Search in Google Chrome prior to 120.0.6099.62 allowed a remote attacker who convinced a user to interact with a malicious file to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: High)
CVE-2023-6510	Use after free in Media Capture in Google Chrome prior to 120.0.6099.62 allowed a remote attacker who convinced a user to interact with a malicious file to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium)
CVE-2023-6511	Inappropriate implementation in Autofill in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-6512	Inappropriate implementation in Web Browser UI in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)
CVE-2023-6702	Type confusion in V8 in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6703	Use after free in Blink in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6704	Use after free in libavif in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6705	Use after free in WebRTC in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6706	Use after free in FedCM in Google Chrome prior to 120.0.6099.109 allowed a remote attacker who convinced a user to interact with a malicious file to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

CVE-2023-6707	Use after free in CSS in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap overflow (Chromium security severity: Medium)
CVE-2024-0406	A flaw was discovered in the mholt/archiver package. This flaw allows an attacker to create a specially crafted tar file to restrict files or directories. This issue can allow the creation or overwriting of files with the user's or application's permissions.
CVE-2024-0853	curl inadvertently kept the SSL session ID for connections in its cache even when the verify status (*OCSP stapling) was disabled. The same hostname could then succeed if the session ID cache was still fresh, which then skipped the verify status check.
CVE-2024-2004	When a protocol selection parameter option disables all protocols without adding any then the default set of protocols is used. This error in the logic for removing protocols. The below command would perform a request to curl.se with a plaintext payload. curl --proto -all,-http http://curl.se The flaw is only present if the set of selected protocols disables the entire set of protocols. There is no practical use and therefore unlikely to be encountered in real situations. The curl security team has thus assessed this as a low severity issue.
CVE-2024-23334	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. When using aiohttp as a web server, it is necessary to specify the root path for static files. Additionally, the option 'follow_symlinks' can be used to determine if following symlinks outside the static root directory. When 'follow_symlinks' is set to True, there is no validation to check if reading a file leads to directory traversal vulnerabilities, resulting in unauthorized access to arbitrary files on the system, even when 'follow_symlinks' and using a reverse proxy are encouraged mitigations. Version 3.9.2 fixes this issue.
CVE-2024-23829	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Security-sensitive parts of the parser are in allowable character sets, that must trigger error handling to robustly match frame boundaries of proxies in order to process requests. Additionally, validation could trigger exceptions that were not handled consistently with processing of other internet standards require could, depending on deployment environment, assist in request smuggling. The unhandled exceptions could lead to consumption on the application server and/or its logging facilities. This vulnerability exists due to an incomplete fix for this vulnerability.
CVE-2024-2466	libcurl did not check the server certificate of TLS connections done to a host specified as an IP address, when built with --enable-ssl. To avoid using the set hostname function when the specified hostname was given as an IP address, therefore completely bypassing all uses of TLS protocols (HTTPS, FTPS, IMAPS, POP3S, SMTPS, etc).
CVE-2024-24788	A malformed DNS message in response to a query can cause the Lookup functions to get stuck in an infinite loop.
CVE-2024-24790	The various Is methods (IsPrivate, IsLoopback, etc) did not work as expected for IPv4-mapped IPv6 addresses, returning false in their traditional IPv4 forms.
CVE-2024-24791	The net/http HTTP/1.1 client mishandled the case where a server responds to a request with an "Expect: 100-continue" header (higher) status. This mishandling could leave a client connection in an invalid state, where the next request sent on the connection to a net/http/httputil.ReverseProxy proxy can exploit this mishandling to cause a denial of service by sending a request that elicit a non-informational response from the backend. Each such request leaves the proxy with an invalid connection that connection to fail.
CVE-2024-25128	Flask-AppBuilder is an application development framework, built on top of Flask. When Flask-AppBuilder is set to use OpenID Connect, an attacker to forge an HTTP request, that could deceive the backend into using any requested OpenID service. This could lead to unauthorized privilege access if a custom OpenID service is deployed by the attacker and accessible by the backend. The application is using the OpenID 2.0 authorization protocol. Upgrade to Flask-AppBuilder 4.3.11 to fix the vulnerability.
CVE-2024-27289	pgx is a PostgreSQL driver and toolkit for Go. Prior to version 4.18.2, SQL injection can occur when all of the following conditions are met: the simple protocol is used; a placeholder for a numeric value must be immediately preceded by a minus; there must be a placeholder for a string value; the first placeholder; both must be on the same line; and both parameter values must be user-controlled. The problem is fixed in v4.18.2 and v5.5.4. As a workaround, reject user input large enough to cause a single query or bind message.
CVE-2024-27304	pgx is a PostgreSQL driver and toolkit for Go. SQL injection can occur if an attacker can cause a single query or bind message. An integer overflow in the calculated message size can cause the one large message to be sent as multiple messages until the connection is closed. This is resolved in v4.18.2 and v5.5.4. As a workaround, reject user input large enough to cause a single query or bind message.
CVE-2024-27306	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. A XSS vulnerability exists on its static file server. This vulnerability is fixed in 3.9.4. We have always recommended using a reverse proxy server (e.g. nginx) for serving static files. These recommendations are unaffected. Other users can disable 'show_index' if unable to upgrade.
CVE-2024-28757	libexpat through 2.6.1 allows an XML Entity Expansion attack when there is isolated use of external parsers (created by the application).
CVE-2024-30251	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. In affected versions an attacker could cause a denial of service (DoS) by sending a form-data request. When the aiohttp server processes it, the server will enter an infinite loop and be unable to process further requests. The application from serving requests after sending a single request. This issue has been addressed in version 3.9.4. Users of affected versions may manually apply a patch to their systems. Please see the linked GHSA for instructions.
CVE-2024-37568	lepture Authlib before 1.3.1 has algorithm confusion with asymmetric public keys. Unless an algorithm is specified in the request, it is allowed with any asymmetric public key. (This is similar to CVE-2022-29217 and CVE-2024-33663.)
CVE-2024-39705	NLTK through 3.8.1 allows remote code execution if untrusted packages have pickled Python code, and the integrity check is not used. This affects, for example, averaged_perceptron_tagger and punkt.

CVE-2024-43796	Express.js minimalist web framework for node. In express < 4.20.0, passing untrusted user input - even after sanitization - to <code>res.render()</code> can result in untrusted code. This issue is patched in express 4.20.0.
CVE-2024-6197	libcurl's ASN1 parser has this <code>utf8asn1str()</code> function used for parsing an ASN.1 UTF-8 string. It can detect an invalid UTF-8 string and abort, but when doing so it also invokes <code>free()</code> on a 4 byte localstack buffer. Most modern malloc implementations detect this error and abort, but some do not. If they do not, they will accept the input pointer and add that memory to its list of available chunks. This leads to the overwriting of nearby memory. The outcome of this is decided by the <code>free()</code> implementation; likely to be memory pointers and a set of flags. The most likely outcome is a crash. This issue can be ruled out that more serious results can be had in special circumstances.
CVE-2024-6874	libcurl's URL API function <code>[curl_url_get()](https://curl.se/libcurl/c/curl_url_get.html)</code> offers punycode conversions for internationalized domain names that is exactly 256 bytes, libcurl ends up reading outside of a stack based buffer when built to use the <code>*macidn* IDN engine</code> . This can lead to reading up the provided buffer exactly - but does not null terminate the string. This flaw can lead to stack contents accidentally being used in the string.
CVE-2024-8986	The grafana plugin SDK bundles build metadata into the binaries it compiles; this metadata includes the repository URL. If credentials are included in the repository URI (for instance, to allow for federated authentication), the resulting binary will contain the full URI, including said credentials.
CVE-2024-9355	A vulnerability was found in Golang FIPS OpenSSL. This flaw allows a malicious user to randomly cause an uninitiated buffer to be returned in FIPS mode. It may also be possible to force a false positive match between non-equal hashes. This is a result of a sum to an untrusted input sum if an attacker can send a zeroed buffer in place of a pre-computed sum. It is also possible to force a false positive match instead of an unpredictable value. This may have follow-on implications for the Go TLS stack.
DLA-3867-1	git - security update
DLA-3878-1	libxml2 - security update
DLA-3881-1	aom - security update
DSA-5746-1	postgresql-13 - security update
GHSA-5cpq-8wj7-hf2v	pyca/cryptography's wheels include a statically linked copy of OpenSSL. The versions of OpenSSL included in cryptography's wheels are vulnerable to a security issue. More details about the vulnerability itself can be found in https://www.openssl.org/news/secadv/20240401.txt . If you are using source ("sdist") then you are responsible for upgrading your copy of OpenSSL. Only users installing from wheels built by cryptography need to update their cryptography versions.
GHSA-7jwh-3vrq-q3m8	### Impact SQL injection can occur if an attacker can cause a single query or bind message to exceed 4 GB in size. This can be done by sending a message size can cause the one large message to be sent as multiple messages under the attacker's control. ### Patches Patched in 1.3.7. ### Workarounds Reject user input large enough to cause a single query or bind message to exceed 4 GB in size.
GHSA-9763-4f94-gfch	### Impact On some platforms, when an attacker can time decapsulation of Kyber on forged cipher texts, they could cause a denial of service. Does not apply to ephemeral usage, such as when used in the regular way in TLS. ### Patches Patched in 1.3.7. ### Workarounds kyberslash.cr.yp.to/)
GHSA-mh55-gqvz-xfwm	Middleware causes a prohibitive amount of heap allocations when processing malicious preflight requests that include a large number of commas in the (ACRH) header whose value contains many commas. This behavior can be abused by attackers to produce undue load and cause a denial of service.
GHSA-mhpq-9638-x6pw	An attacker controlled input of a PBES2 encrypted JWE blob can have a very large p2c value that, when decrypted, causes a denial of service.
GHSA-pjjw-qhg8-p2p9	### Summary llhttp 8.1.1 is vulnerable to two request smuggling vulnerabilities. Details have not been disclosed yet. The issue is resolved by using llhttp 9+ (which is included in aiohttp 3.8.6+).
RHBA-2024:5691	The ca-certificates package contains a set of Certificate Authority (CA) certificates chosen by the Mozilla Foundation for use in the Internet Infrastructure (PKI).
RHSA-2023:0050	Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
RHSA-2023:0095	The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.
RHSA-2023:0096	D-Bus is a system for sending messages between applications. It is used both for the system-wide message bus service and for inter-process communication messaging facility.
RHSA-2023:0100	The systemd packages contain systemd, a system and service manager for Linux, compatible with the SysV and LSB init systems. It provides parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemons, supports Linux cgroups. In addition, it supports snapshotting and restoring of the system state, maintains mount and automount units, and transactional dependency-based service control logic. It can also work as a drop-in replacement for sysvinit.
RHSA-2023:0103	Expat is a C library for parsing XML documents.
RHSA-2023:0116	A library that provides Abstract Syntax Notation One (ASN.1, as specified by the X.680 ITU-T recommendation) and Distinguished Encoding Rules (DER, as per X.690) encoding and decoding functions.
RHSA-2023:0173	The libxml2 library is a development toolbox providing the implementation of various XML standards.
RHSA-2023:0379	X.Org X11 libXpm runtime library.

RHSA-2023:0610	Git is a distributed revision control system with a decentralized architecture. As opposed to centralized version control systems, Git ensures that each working copy of a Git repository is an exact copy with complete revision history. This not only allows for distributed projects without the need to have permission to push the changes to their official repositories, but also makes it possible to work offline.
RHSA-2023:0625	KSBA (pronounced Kasbah) is a library to make X.509 certificates as well as the CMS easily accessible by other applications. It supports blocks of S/MIME and TLS.
RHSA-2023:0833	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems.
RHSA-2023:0835	The python-setuptools package provides a collection of enhancements to Python distribution utilities allowing convenient installation of packages.
RHSA-2023:0837	The systemd packages contain systemd, a system and service manager for Linux, compatible with the SysV and LSB init systems. It has parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemons, and Linux cgroups. In addition, it supports snapshotting and restoring of the system state, maintains mount and automount units, and transactional dependency-based service control logic. It can also work as a drop-in replacement for sysvinit.
RHSA-2023:0842	The GNU tar program can save multiple files in an archive and restore files from an archive.
RHSA-2023:0852	The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server.
RHSA-2023:1405	OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols and a general cryptography library.
RHSA-2023:1569	The gnutls packages provide the GNU Transport Layer Security (GnuTLS) library, which implements cryptographic protocols such as TLS, and DTLS.
RHSA-2023:1673	The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server.
RHSA-2023:1743	Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
RHSA-2023:1930	GNU Emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a mail client, and a way to read e-mail and news.
RHSA-2023:2076	The libwebp packages provide a library and tools for the WebP graphics format. WebP is an image format with a lossy and lossless mode. Images. WebP consists of a codec based on the VP8 format, and a container based on the Resource Interchange File Format. Developers and browser developers can use WebP to compress, archive, and distribute digital images more efficiently.
RHSA-2023:2763	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems.
RHSA-2023:2859	Git is a distributed revision control system with a decentralized architecture. As opposed to centralized version control systems, Git ensures that each working copy of a Git repository is an exact copy with complete revision history. This not only allows for distributed projects without the need to have permission to push the changes to their official repositories, but also makes it possible to work offline.
RHSA-2023:2883	The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.
RHSA-2023:2951	The kernel packages contain the Linux kernel, the core of any Linux operating system.
RHSA-2023:3018	The libarchive programming library can create and read several different streaming archive formats, including GNU tar, zip, and bzip2. Libarchive is used notably in the bsdtar utility, scripting language bindings such as python-libarchive, and several Perl modules.
RHSA-2023:3042	GNU Emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a mail client, and a way to read e-mail and news.
RHSA-2023:3104	GNU Emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a mail client, and a way to read e-mail and news.
RHSA-2023:3109	The Apache Portable Runtime (APR) is a portability library used by the Apache HTTP Server.
RHSA-2023:3246	Git is a distributed revision control system with a decentralized architecture. As opposed to centralized version control systems, Git ensures that each working copy of a Git repository is an exact copy with complete revision history. This not only allows for distributed projects without the need to have permission to push the changes to their official repositories, but also makes it possible to work offline.
RHSA-2023:3781	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems.
RHSA-2023:3827	The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.
RHSA-2023:5050	The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server.
RHSA-2023:5244	The kernel packages contain the Linux kernel, the core of any Linux operating system.

RHSA-2023:5309	The libwebp packages provide a library and tools for the WebP graphics format. WebP is an image format with a lossy and lossless image format. WebP consists of a codec based on the VP8 format, and a container based on the Resource Interchange File Format (RIFF). WebP developers and browser developers can use WebP to compress, archive, and distribute digital images more efficiently.
RHSA-2023:5353	The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.
RHSA-2023:6236	The binutils packages provide a collection of binary utilities for the manipulation of object code in various object formats. The utilities include nm, objcopy, objdump, ranlib, readelf, size, strings, strip, and addr2line utilities.
RHSA-2023:7029	The libX11 packages contain the core X11 protocol client library.
RHSA-2023:7050	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems.
RHSA-2023:7077	The kernel packages contain the Linux kernel, the core of any Linux operating system.
RHSA-2023:7165	The Common UNIX Printing System (CUPS) provides a portable printing layer for Linux, UNIX, and similar operating systems.
RHSA-2023:7190	Avahi is an implementation of the DNS Service Discovery and Multicast DNS specifications for Zero Configuration Networking on a local network. Avahi and Avahi-aware applications allow you to plug your computer into a network and, without the need for a DHCP server, view printers to print with, and find shared files on other computers.
RHSA-2023:7549	The kernel packages contain the Linux kernel, the core of any Linux operating system.
RHSA-2023:7836	Avahi is an implementation of the DNS Service Discovery and Multicast DNS specifications for Zero Configuration Networking on a local network. Avahi and Avahi-aware applications allow you to plug your computer into a network and, without the need for a DHCP server, view printers to print with, and find shared files on other computers.
RHSA-2024:0105	Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security applications and services.
RHSA-2024:0113	The kernel packages contain the Linux kernel, the core of any Linux operating system.
RHSA-2024:0265	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit.
RHSA-2024:0965	The unbound packages provide a validating, recursive, and caching DNS or DNSSEC resolver.
RHSA-2024:1751	The unbound packages provide a validating, recursive, and caching DNS or DNSSEC resolver.
RHSA-2024:1786	The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server.
RHSA-2024:1818	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit.
RHSA-2024:2973	The libX11 packages contain the core X11 protocol client library.
RHSA-2024:2974	X.Org X11 libXpm runtime library.
RHSA-2024:3059	The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.
RHSA-2024:3121	The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server.
RHSA-2024:3138	The kernel packages contain the Linux kernel, the core of any Linux operating system.
RHSA-2024:3618	The kernel packages contain the Linux kernel, the core of any Linux operating system.
RHSA-2024:5529	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols.
RHSA-2024:6166	Kerberos is a network authentication system, which can improve the security of your network by eliminating the need for a network in unencrypted form. It allows clients and servers to authenticate to each other with the help of a trusted third party (KDC).
RHSA-2024:6969	The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runC.
RHSA-2024:7135	Git Large File Storage (LFS) replaces large files such as audio samples, videos, datasets, and graphics with text pointers to files on a remote server.