CDP Private Cloud Data Services 1.5.4

CDP Private Cloud Data Services Release Notes

Date published: 2023-12-16
Date modified: 2024-05-30

https://docs.cloudera.com/

Legal Notice

Contents

Data Services Release Notes

CDP Private Cloud Data Services includes the Management Console, Cloudera Data Warehouse (CDW), Cloudera Machine Learning (CML) and Cloudera Data Engineering (CDE). Learn about the new features and improvements in each of these services.

New features in Platform

Certifications

- CDP Private Cloud Base (7.1.9 CHF 6, 7.1.7 SP3, 7.1.8 CHF22)
- Cloudera Manager 7.11.3 CHF 6
- 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, CDW, and 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.

New features in Cloudera Data Engineering

Support for password protected private key to initialize the virtual cluster

You can now use the password protected private keys to initialize the virtual cluster. Currently, the password protected private keys are supported with RSA and EC algorithms only. For more information, see Initializing virtual clusters.

Support for Spark Connect session (Preview)

CDE supports Spark Connect sessions which are a type of CDE sessions that expose the Spark Connect interface and allows you to run spark commands from any remote Python environment.

New features in Cloudera Data Warehouse

Hue supports natural language query processing (Preview)

Hue leverages the power of Large Language Models (LLM) to help you generate SQL queries from natural language prompts and also provides options to optimize, explain, and fix queries, promoting efficient and accurate practices for accessing and manipulating data. You can use several

AI services and models such as OpenAI's GPT service, Amazon Bedrock, and Azure's OpenAI service to run the Hue SQL AI assistant.

- To learn more about the supported models and services, limitations, and what data is shared with the LLMs, see About the SQL AI Assistant in CDW.
- To set up and enable the SQL AI Assistant, see About setting up the SQL AI Assistant in CDW.
- To see how to generate, edit, explain, optimize, and fix queries, see Starting the SQL AI Assistant in Hue.

Improvements to custom pod configuration (now known as Resource Templates)

Several improvements and changes have been made to the custom pod configuration functionality starting with CDP Private Cloud Data Services 1.5.4. The custom pod configuration has been renamed to "Resource Templates".

- A new menu option Resource Templates has been added to the left navigation pane on the CDW web interface.
- You can now configure the allocation of Kubernetes resources to the pods for Hive, Data Visualization, and Database Catalog in addition to Impala.
- The Impala pod configuration feature is moved from the **Environment Details** page to the **Resource Templates** page.

For more information, see Resource templates for CDW Private Cloud pods.

Flexibility to enable and disable quota management for CDW entities

Earlier, you were required to enable the quota management option before activating an environment to use quota-managed resource pools for environments, Data Catalogs, Virtual Warehouses, and Data Visualization instances in CDW. Starting with CDP Private Cloud Data Services 1.5.4, you can enable or disable the quota management option at any time during the lifecycle of the CDW entities. To learn more about the behavioral aspects, see Quota Management in CDW Private Cloud.

Added support for authentication between CDW and HMS database using mTLS

CDW and the Hive MetaStore (HMS) database on the base cluster can mutually authenticate each other during the SSL/TLS handshake using mTLS for all supported backend databases (Oracle, MySQL, MariaDB, and Postgres). To set up mTLS, you must upload the database client certificate and the private key files in PEM format while activating an environment in CDW. See Enabling mTLS between the HMS database and CDW on Private Cloud.

Ability to enable active-passive configuration for HiveServer2 pods

CDW provides an option to enable active-passive configuration for HiveServer2 (HS2) pods in Private Cloud. By enabling this feature, two HS2 pods run simultaneously–one active and the other inactive. When one pod terminates, the inactive pod becomes active, providing High Availability. See HiveServer2 High Availability in CDW Private Cloud. The most likely cause of a pod's termination is node failure.

CDW no longer has a dependency on YARN

Environment activation in CDW no longer depends on or fails if the YARN service is not installed on the CDP Base cluster.

Improvements to backup and restore CDW

There are two ways to create backups of the Data Warehosue service:

- Using Data Recovery Service (DRS)
- Using the CDW's CDP CLI cluster management commands

By default, CDW backs up namespace-related data before starting the upgrade process using the Data Recovery Service (DRS). A new option called Back up Virtual Warehouse namespaces before an upgrade has been added to disable the automatic backup process on the Advanced Configuration page in the CDW web interface.

New features in Cloudera Machine Learning

CML Service Accounts are available in CML Private Cloud

In CML, the Kerberos principal for the Service Account may not be the same as your login information. Therefore, ensure you provide the Kerberos identity when you sign in to the Service Account. For more information, see Authenticating Hadoop for CML Service Accounts.

Model Registry is available in CDP Private Cloud

Model Registry is now generally available (GA) in CDP Private Cloud. Model Registry in CDP Private Cloud uses Apache Ozone to store model artifacts. For creating a Model Registry you need the Ozone S3 gateway endpoint, the Ozone access key, and the Ozone secret key. If you deploy Model Registry in an environment that contains one or more CML workspaces, you must synchronize the Model Registry with the workspaces. For more information, see Prerequisites for creating Model Registry and Synchronizing the model registry with a workspace.

Heterogeneous GPU usage

When using heterogeneous GPU clusters to run sessions and jobs, the available GPU accelerator labels need to be selected during workload creation. For more information, see Heterogeneous GPU clusters.

Data connections without auto discovery

Cloudera Machine Learning is a flexible, open platform, supporting connections to many data sources. The provided code samples demonstrate how to access local data for CML workloads. For more information, see Connecting to CDW.

Spark Log4j Configuration

Cloudera Machine Learning allows you to update Spark's internal logging configuration on a per-project basis. Spark logging properties can be customized for every session, and job with a default file path found at the root of your project. You can also specify a custom location with a custom environment variable. For more information, see Spark Log4j Configuration.

ML Metrics Collector service

The Metrics Collector service gathers data about how users and groups use resource quota, like how much CPU, Memory and GPU capacity (if any) is allocated, and what the users or groups utilize from that. The Metrics Collector service is running by default, but to collect data about resource quota metrics, you need to enable the Quota Management feature. For more information, see ML Metrics Collector Service overview.

Quota Management for group level (Preview)

Quota Management Technical Preview (TP) release enables you to control how resources are allocated within your CML workspace on user and on group level. Yunikorn Gang Scheduling is also available, which is the default scheduling mechanism in Cloudera Machine Learning. For more information, see Quota Management overview and Yunikorn Gang Scheduling.

Restarting a failed AMP setup

You can now retry failed AMP deployment steps and continue the AMP setup to handle intermittent and configuration issues. For more information, see Restarting a failed AMP setup.

New Hadoop CLI Runtime Addon versions are available

The HadoopCLI 7.1.8.3-601 Runtime Addon is released for the Private Cloud.

Release notes for component services

- Data Catalog
- Management Console
- Cloudera Data Warehouse (CDW)
- Cloudera Machine Learning (CML)
- Cloudera Data Engineering (CDE)
- Cloudera Manager

- Replication Manager

List of fixed Common Vulnerabilities and Exposures

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
- CVE-2024-33870
- CVE-2024-33869
- CVE-2024-29510
- DSA-5679-1: less - security update
- DSA-5682-2
- 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 <=0.9.2 and DuckDB extension-template <=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 writingJavaScript. 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 nghttp2 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 parsingcomponent 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 Rackto take an unexpected amount of time, possibly resulting in a denial ofservice attack vector. This header is used typically used in multipartparsing. Any applications that parse multipart posts using Rack (virtuallyall 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 tocraft 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) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.

  The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.

  The consequences of this kind of internal application state corruption canbe various - from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.

  The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.

  As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The 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 xmlSnprintfElementContent 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/openldap/generate-server-cert.sh in openldap-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 unscape 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.

- RHSA-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.
- RHSA-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 `encodeurl`](https://github.com/pillarjs/encodeurl) 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 scalers, 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 differentalgorithms. The number of acceptable "links" in this "decompression chain" wascapped, but the cap was implemented on a per-header basis allowing a maliciousserver to insert a virtually unlimited number of compression steps simply byusing 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 callows 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 offical 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`, `sslhostnameverifier`, `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_tempdir, and make_tempname 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: his 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.

  Please 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-2021-46310: 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
- 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.