Vulnerability Report Document

Document Information

Date: 2025-01-15T10:00:00Z

Tools:
- grype (0.91.0)

Component name : Test Application (1.0.0)

BOM Format: CycloneDX
Specification Version: 1.5
Version: 1
Serial Number: urn:uuid:439fe70b-a94d-448f-ae65-b6412c812a2f

Vulnerabilities

1. ID: **CVE-2025-27152**
   Description: axios is a promise based HTTP client for the browser and node.js. The issue occurs when passing absolute URLs rather than protocol-relative URLs to axios. Even if □baseURL is set, axios sends the request to the specified absolute URL, potentially causing SSRF and credential leakage. This issue impacts both server-side and client-side usage of axios. This issue is fixed in 1.8.2.

   - **Severity:** high (other)

   Affected Document Components : [*axios*: 1.7.9 **]**

2. ID: **GHSA-jr5f-v2jv-69x6**
   Description: axios Requests Vulnerable To Possible SSRF and Credential Leakage via Absolute URL

   - **Severity:** high (other)

   Affected Document Components : [*axios*: 1.7.9 **]**

3. ID: **CVE-2016-9840**
   Description: inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.

   - **Severity:** high (CVSSv31)
   - **Severity:** high (CVSSv2)

   Affected Document Components : [*boost*: 1.75.0 **]**

4. ID: **CVE-2023-33953**
   Description: gRPC contains a vulnerability that allows hpack table accounting errors could lead to unwanted disconnects between clients and servers in exceptional cases/ Three vectors were found that allow the following DOS attacks:
   - Unbounded memory buffering in the HPACK parser
   - Unbounded CPU consumption in the HPACK parser
   The unbounded CPU consumption is down to a copy that occurred per-input-block in the parser, and because that could be unbounded 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 buffering bugs:
   - The header size limit check was behind the string reading code, so we needed to first buffer up to a 4 gigabyte string before rejecting it as longer than 8 or 16kb.
   - HPACK varints have an encoding quirk whereby an infinite number of 0's can be added at the start of an integer. gRPC's hpack parser needed to read all of them before concluding a parse.

- gRPC's metadata overflow check was performed per frame, so that the following sequence of frames could cause infinite buffering: HEADERS: containing a: 1 CONTINUATION: containing a: 2 CONTINUATION: containing a: 3 etc…

  - **Severity:** high (CVSSv31)
  - **Severity:** high (CVSSv31)

Affected Document Components : [*grpc*: 1.35.0 **]**

5. ID: **CVE-2023-44487**
   Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

   - **Severity:** high (CVSSv31)
   - **Severity:** high (CVSSv31)

   Affected Document Components : [*grpc*: 1.35.0 **]**

6. ID: **CVE-2023-4785**
   Description: Lack of error handling in the TCP server in Google's gRPC starting version 1.23 on posix-compatible platforms (ex. Linux) allows an attacker to cause a denial of service by initiating a significant number of connections with the server. Note that gRPC C++ Python, and Ruby are affected, but gRPC Java, and Go are NOT affected.

   - **Severity:** high (CVSSv31)
   - **Severity:** high (CVSSv31)

   Affected Document Components : [*grpc*: 1.35.0 **]**

7. ID: **CVE-2023-32732**
   Description: gRPC contains a vulnerability whereby a client can cause a termination of connection between a HTTP2 proxy and a gRPC server: a base64 encoding error for `-bin` suffixed headers will result in a disconnection by the gRPC server, but is typically allowed by HTTP2 proxies. We recommend upgrading beyond the commit in https://github.com/grpc/grpc/pull/32309 https://www.google.com/url

   - **Severity:** medium (CVSSv31)
   - **Severity:** medium (CVSSv31)

   Affected Document Components : [*grpc*: 1.35.0 **]**

8. ID: **GHSA-64vf-vj9q-5phr**
   Description: Malware in icons-material

   - **Severity:** critical (other)

   Affected Document Components : [*icons-material*: 5.16.4 **]**

9. ID: **GHSA-9c47-m6qq-7p4h**
   Description: Prototype Pollution in JSON5 via Parse Method

   - **Severity:** high (CVSSv31)

   Affected Document Components : [*json5*: 0.9.11 **]**

10. ID: **CVE-2024-43805**
    Description: jupyterlab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook Architecture. This vulnerability depends on user interaction by opening a malicious notebook with Markdown cells, or Markdown file using JupyterLab preview feature. A malicious user can access any data that the attacked user has access to as well as perform arbitrary requests acting as the attacked user. JupyterLab

v3.6.8, v4.2.5 and Jupyter Notebook v7.2.2 have been patched to resolve this issue. Users are advised to upgrade. There is no workaround for the underlying DOM Clobbering susceptibility. However, select plugins can be disabled on deployments which cannot update in a timely fashion to minimise the risk. These are: 1. `@jupyterlab/mathjax-extension:plugin` - users will loose ability to preview mathematical equations. 2. `@jupyterlab/markdownviewer-extension:plugin` - users will loose ability to open Markdown previews. 3. `@jupyterlab/mathjax2-extension:plugin` (if installed with optional `jupyterlab-mathjax2` package) - an older version of the mathjax plugin for JupyterLab 4.x. To disable these extensions run: ```jupyter labextension disable @jupyterlab/markdownviewer-extension:plugin && jupyter labextension disable @jupyterlab/mathjax-extension:plugin && jupyter labextension disable @jupyterlab/mathjax2-extension:plugin ``` in bash.

- **Severity:** medium (CVSSv31)
- **Severity:** medium (CVSSv31)

Affected Document Components : [*notebook*: 7.0.7 **]**

11. ID: **CVE-2021-32024**
Description: A remote code execution vulnerability in the BMP image codec of BlackBerry QNX SDP version(s) 6.4 to 7.1 could allow an attacker to potentially execute code in the context of the affected process.

- **Severity:** critical (CVSSv31)
- **Severity:** critical (CVSSv2)

Affected Document Components : [*qnx_software_development_platform*: 7.1 **]**

12. ID: **CVE-2024-48856**
Description: Out-of-bounds write in the PCX image codec in QNX SDP versions 8.0, 7.1 and 7.0 could allow an unauthenticated attacker to cause a denial-of-service condition or execute code in the context of the process using the image codec.

- **Severity:** critical (CVSSv31)
- **Severity:** critical (CVSSv31)

Affected Document Components : [*qnx_software_development_platform*: 7.1 **]**

13. ID: **CVE-2013-2687**
Description: Stack-based buffer overflow in the bpe_decompress function in (1) BlackBerry QNX Neutrino RTOS through 6.5.0 SP1 and (2) QNX Momentics Tool Suite through 6.5.0 SP1 in the QNX Software Development Platform allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted packets to TCP port 4868.

- **Severity:** high (CVSSv2)

Affected Document Components : [*qnx_software_development_platform*: 7.1 **]**

14. ID: **CVE-2023-32701**
Description: Improper Input Validation in the Networking Stack of QNX SDP version(s) 6.6, 7.0, and 7.1 could allow an attacker to potentially cause Information Disclosure or a Denial-of-Service condition.

- **Severity:** high (CVSSv31)
- **Severity:** high (CVSSv31)

Affected Document Components : [*qnx_software_development_platform*: 7.1 **]**

15. ID: **CVE-2024-48854**
Description: Off-by-one error in the TIFF image codec in QNX SDP versions 8.0, 7.1 and 7.0 could allow an unauthenticated attacker to cause an information disclosure in the context of the process using the image codec.

- **Severity:** high (CVSSv31)

Severity: high (CVSSv31)

Affected Document Components : [*qnx_software_development_platform*: 7.1 **]**

16. ID: **CVE-2024-48855**
Description: Out-of-bounds read in the TIFF image codec in QNX SDP versions 8.0, 7.1 and 7.0 could allow an unauthenticated attacker to cause an information disclosure in the context of the process using the image codec.

- **Severity:** high (CVSSv31)
- **Severity:** high (CVSSv31)

Affected Document Components : [*qnx_software_development_platform*: 7.1 **]**

17. ID: **CVE-2024-48857**
Description: NULL pointer dereference in the PCX image codec in QNX SDP versions 8.0, 7.1 and 7.0 could allow an unauthenticated attacker to cause a denial-of-service condition in the context of the process using the image codec.

- **Severity:** high (CVSSv31)
- **Severity:** high (CVSSv31)

Affected Document Components : [*qnx_software_development_platform*: 7.1 **]**

18. ID: **CVE-2013-2688**
Description: Buffer overflow in phrelay in BlackBerry QNX Neutrino RTOS through 6.5.0 SP1 in the QNX Software Development Platform allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted packets to TCP port 4868 that leverage improper handling of the /dev/photon device file.

- **Severity:** medium (CVSSv2)

Affected Document Components : [*qnx_software_development_platform*: 7.1 **]**

19. ID: **CVE-2024-6345**
Description: A vulnerability in the package_index module of pypa/setuptools versions up to 69.1.1 allows for remote code execution via its download functions. These functions, which are used to download packages from URLs provided by users or retrieved from package index servers, are susceptible to code injection. If these functions are exposed to user-controlled inputs, such as package URLs, they can execute arbitrary commands on the system. The issue is fixed in version 70.0.

- **Severity:** high (CVSSv3)

Affected Document Components : [*setuptools*: 63.2.0 **]**

20. ID: **CVE-2022-40897**
Description: Python Packaging Authority (PyPA) setuptools before 65.5.1 allows remote attackers to cause a denial of service via HTML in a crafted package or custom PackageIndex page. There is a Regular Expression Denial of Service (ReDoS) in package_index.py.

- **Severity:** medium (CVSSv31)
- **Severity:** medium (CVSSv31)

Affected Document Components : [*setuptools*: 63.2.0 **]**

21. ID: **CVE-2025-3277**
Description: An integer overflow can be triggered in SQLite's `concat_ws()` function. The resulting, truncated integer is then used to allocate a buffer. When SQLite then writes the resulting string to the buffer, it uses the original, untruncated size and thus a wild Heap Buffer overflow of size ~4GB can be triggered. This can result in arbitrary code execution.

- **Severity:** medium (other)

Affected Document Components : [*sqlite*: 3.45.2 **]**

22. ID: **CVE-2025-29087**
Description: In SQLite 3.44.0 through 3.49.0 before 3.49.1, the concat_ws() SQL function can cause memory to be written beyond the end of a malloc-allocated buffer. If the separator argument is attacker-controlled and has a large string (e.g., 2MB or more), an integer overflow occurs in calculating the size of the result buffer, and thus malloc may not allocate enough memory.

- **Severity:** low (CVSSv31)

Affected Document Components : [*sqlite*: 3.45.2 **]**

23. ID: **CVE-2023-29159**
Description: Directory traversal vulnerability in Starlette versions 0.13.5 and later and prior to 0.27.0 allows a remote unauthenticated attacker to view files in a web service which was built using Starlette.

- **Severity:** high (CVSSv31)
- **Severity:** high (CVSSv31)

Affected Document Components : [*starlette*: 0.17.1 **]**

24. ID: **CVE-2023-30798**
Description: There MultipartParser usage in Encode's Starlette python framework before versions 0.25.0 allows an unauthenticated and remote attacker to specify any number of form fields or files which can cause excessive memory usage resulting in denial of service of the HTTP service.

- **Severity:** high (CVSSv31)
- **Severity:** high (CVSSv31)

Affected Document Components : [*starlette*: 0.17.1 **]**

25. ID: **CVE-2024-47874**
Description: Starlette is an Asynchronous Server Gateway Interface (ASGI) framework/toolkit. Prior to version 0.40.0, Starlette treats `multipart/form-data` parts without a `filename` as text form fields and buffers those in byte strings with no size limit. This allows an attacker to upload arbitrary large form fields and cause Starlette to both slow down significantly due to excessive memory allocations and copy operations, and also consume more and more memory until the server starts swapping and grinds to a halt, or the OS terminates the server process with an OOM error. Uploading multiple such requests in parallel may be enough to render a service practically unusable, even if reasonable request size limits are enforced by a reverse proxy in front of Starlette. This Denial of service (DoS) vulnerability affects all applications built with Starlette (or FastAPI) accepting form requests. Verison 0.40.0 fixes this issue.

- **Severity:** high (other)

Affected Document Components : [*starlette*: 0.17.1 **]**

26. ID: **GHSA-72xf-g2v4-qvf3**
Description: tough-cookie Prototype Pollution vulnerability

- **Severity:** medium (CVSSv31)

Affected Document Components : [*tough-cookie*: 4.1.2 **]**

27. ID: **GHSA-j8xg-fqg3-53r7**
Description: word-wrap vulnerable to Regular Expression Denial of Service

- **Severity:** medium (CVSSv31)

Affected Document Components : [*word-wrap*: 1.2.3 **]**

28. ID: **GHSA-3h5v-q93c-6h6q**
Description: ws affected by a DoS when handling a request with many HTTP headers

- **Severity:** high (CVSSv31)

Affected Document Components : [*ws*: 8.13.0 **]**

Components

Name: *axios*
Version: 1.7.9

Name: *boost*
Version: 1.75.0

Name: *grpc*
Version: 1.35.0

Name: *icons-material*
Version: 5.16.4

Name: *json5*
Version: 0.9.11

Name: *notebook*
Version: 7.0.7

Name: *qnx_software_development_platform*
Version: 7.1

Name: *setuptools*
Version: 63.2.0

Name: *sqlite*
Version: 3.45.2

Name: *starlette*
Version: 0.17.1

Name: *tough-cookie*
Version: 4.1.2

Name: *word-wrap*
Version: 1.2.3

Name: *ws*
Version: 8.13.0

Name: *lodash*
Version: 4.17.21

Name: *express*
Version: 4.18.2

Name: *numpy*
Version: 1.24.0