Vulnerability Report Document

Document Information

Date: 2025-10-24T10:52:21Z

Tools:
- Dependency-Track (4.13.3)

Component name : another test (0.5.0)

BOM Format: CycloneDX
Specification Version: 1.5
Version: 1
Serial Number: urn:uuid:52a575aa-462b-4259-a0a5-dc55beb7fc77

Vulnerabilities

1. 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:** medium (CVSSv2 — Source: NVD)
   - **Severity:** high (CVSSv3 — Source: NVD)

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

2. ID: **CVE-2025-53628**
   Description: cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.20.1, cpp-httplib does not have a limit for a unique line, permitting an attacker to explore this to allocate memory arbitrarily. This vulnerability is fixed in 0.20.1. NOTE: This vulnerability is related to CVE-2025-53629.

   - **Severity:** high (CVSSv3 — Source: NVD)

   Affected Document Components : [*cpp-httplib*: 0.15.3 **]**

3. ID: **CVE-2025-53629**
   Description: cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.23.0, incoming requests using Transfer-Encoding: chunked in the header can allocate memory arbitrarily in the server, potentially leading to its exhaustion. This vulnerability is fixed in 0.23.0. NOTE: This vulnerability is related to CVE-2025-53628.

   - **Severity:** high (CVSSv3 — Source: NVD)

   Affected Document Components : [*cpp-httplib*: 0.15.3 **]**

4. 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:** high (CVSSv2 — Source: NVD)
   - **Severity:** critical (CVSSv3 — Source: NVD)

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

5. 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 (CVSSv3 — Source: NVD)

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

6. 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 (CVSSv3 — Source: NVD)

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

7. 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 (CVSSv3 — Source: NVD)

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

8. 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 (CVSSv3 — Source: NVD)

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

9. 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 (CVSSv3 — Source: NVD)

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

10. ID: **CVE-2025-47273**
    Description: setuptools is a package that allows users to download, build, install, upgrade, and uninstall Python packages. A path traversal vulnerability in `PackageIndex` is present in setuptools prior to version 78.1.1. An attacker would be allowed to write files to arbitrary locations on the filesystem with the permissions of the process running the Python code, which could escalate to remote code execution depending on the context. Version 78.1.1 fixes the issue.

    - **Severity:** high (CVSSv3 — Source: NVD)

    Affected Document Components : [*setuptools*: 75.3.0 **]**

11. ID: **CVE-2024-50614**
    Description: TinyXML2 through 10.0.0 has a reachable assertion for UINT_MAX/16, that may lead to application exit, in tinyxml2.cpp XMLUtil::GetCharacterRef.

    - **Severity:** medium (CVSSv3 — Source: NVD)

    Affected Document Components : [*tinyxml2*: 10.0.0 **]**

12. ID: **CVE-2024-50615**
    Description: TinyXML2 through 10.0.0 has a reachable assertion for UINT_MAX/digit, that may lead to application exit, in tinyxml2.cpp XMLUtil::GetCharacterRef.

    - **Severity:** medium (CVSSv3 — Source: NVD)

Affected Document Components : [*tinyxml2*: 10.0.0 **]**

13. ID: **CVE-2025-6375**

    Description: A vulnerability was found in poco up to 1.14.1. It has been rated as problematic. Affected by this issue is the function MultipartInputStream of the file Net/src/MultipartReader.cpp. The manipulation leads to null pointer dereference. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 1.14.2 is able to address this issue. The patch is identified as 6f2f85913c191ab9ddfb8fae781f5d66afccf3bf. It is recommended to upgrade the affected component.

    - **Severity:** low (CVSSv2 — Source: NVD)
    - **Severity:** medium (CVSSv3 — Source: NVD)

    Analysis: **In Triage**

    - **Justification:** Requires Configuration

    Affected Document Components : [*poco*: 1.14.0 **]**

14. ID: **CVE-2025-58754**

    Description: Axios is a promise based HTTP client for the browser and Node.js. When Axios prior to versions 0.30.2 and 1.12.0 runs on Node.js and is given a URL with the `data:` scheme, it does not perform HTTP. Instead, its Node http adapter decodes the entire payload into memory (`Buffer`/`Blob`) and returns a synthetic 200 response. This path ignores `maxContentLength` / `maxBodyLength` (which only protect HTTP responses), so an attacker can supply a very large `data:` URI and cause the process to allocate unbounded memory and crash (DoS), even if the caller requested `responseType: 'stream'`. Versions 0.30.2 and 1.12.0 contain a patch for the issue.

    - **Severity:** high (CVSSv3 — Source: NVD)

    Affected Document Components : [*axios*: 1.8.2 **]**

Components

Name: *axios*
Version: 1.8.2

Name: *boost*
Version: 1.75.0

Name: *cpp-httplib*
Version: 0.15.3

Name: *poco*
Version: 1.14.0

Name: *qnx_software_development_platform*
Version: 7.1

Name: *setuptools*
Version: 75.3.0

Name: *tinyxml2*
Version: 10.0.0