TLP:WHITE

VDE-2024-073: Phoenix Contact: Multiple Vulnerabilities in PLCnext Firmware

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Mon Dec 09 12:00:00 CET 2024	Engine: 2.5.15
Current release date: Mon Dec 09 12:00:00 CET 2024	Build Date: Tue Dec 03 09:39:24 CET 2024
Current version: 1	Status: FINAL
CVSSv3.1 Base Score: 9.8	Severity: Critical
Original language: en	Language: en-GB
Also referred to: VDE-2024-073, PCSA-2024/00017	

Summary

Multiple Linux component vulnerabilities fixed in latest PLCnext Firmware release 2024.0.6 LTS

General Recommendation

Phoenix Contact recommends operating network-capable devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note.

Impact

Availability, integrity, or confidentiality of the PLCnext Control might be compromised by attacks using these vulnerabilities.

Remediation

Update to the latest 2024.0.6 LTS Firmware Release. PHOENIX CONTACT recommends to always use an up-to-date version of the PLCnext Engineer.

Product groups

Affected Products.

- Firmware < 2024.0.6 LTS installed on AXC F 1152
- Firmware < 2024.0.6 LTS installed on AXC F 2152
- Firmware < 2024.0.6 LTS installed on AXC F 3152
- Firmware < 2024.0.6 LTS installed on RFC 4072S
- Firmware < 2024.0.6 LTS installed on BPC 9102S
- Firmware < 2024.0.6 LTS installed on RFC 4072R
- Firmware < 2024.0.3 LTS installed on EPC 1502
- Firmware < 2024.0.3 LTS installed on EPC 1522

Fixed Product.

- Firmware 2024.0.6 LTS installed on AXC F 1152
- Firmware 2024.0.6 LTS installed on AXC F 2152
- Firmware 2024.0.6 LTS installed on AXC F 3152
- Firmware 2024.0.6 LTS installed on RFC 4072S
- Firmware 2024.0.6 LTS installed on BPC 9102S
- Firmware 2024.0.6 LTS installed on RFC 4072R
- Firmware 2024.0.3 LTS installed on EPC 1502
- Firmware 2024.0.3 LTS installed on EPC 1522

Vulnerabilities

CVE-2023-38039

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-38039

Vulnerability Description

When curl retrieves an HTTP response, it stores the incoming headers so that they can be accessed later via the libcurl headers API.

However, curl did not have a limit in how many or how large headers it would accept in a response, allowing a malicious server to stream an endless series of headers and eventually cause curl to run out of heap memory.

CWE: CWE-201: Insertion of Sensitive Information Into Sent Data

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-46219

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-46219

Vulnerability Description

When saving HSTS data to an excessively long file name, curl could end up removing all contents, making subsequent requests using that file unaware of the HSTS status they should otherwise use.

CWE: CWE-311: Missing Encryption of Sensitive Data

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-46218

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-46218

Vulnerability Description

This flaw allows a malicious HTTP server to set "super cookies" in curl that are then passed back to more origins than what is otherwise allowed or possible. This allows a site to set cookies that then would get sent to different and unrelated sites and domains.

It could do this by exploiting a mixed case flaw in curl's function that verifies a given cookie domain against the Public Suffix List (PSL). For example a cookie could be set with `domain=co.UK` when the URL used a lower case hostname `curl.co.uk`, even though `co.uk` is listed as a PSL domain.

CWE: CWE-201: Insertion of Sensitive Information Into Sent Data

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-38545

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-38545

Vulnerability Description

This flaw makes curl overflow a heap based buffer in the SOCKS5 proxy handshake.

When curl is asked to pass along the host name to the SOCKS5 proxy to allow that to resolve the address instead of it getting done by curl itself, the maximum length that host name can be is 255 bytes.

If the host name is detected to be longer, curl switches to local name resolving and instead passes on the resolved address only. Due to this 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 host name to the target buffer instead of copying just the resolved address there.

The target buffer being a heap based buffer, and the host name coming from the URL that curl has been told to operate with.

CWE: CWE-787: Out-of-bounds Write

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-38546

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-38546

Vulnerability Description

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 en 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.

CWE: CWE-73: External Control of File Name or Path

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N	3.7
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N	3.7
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N	3.7
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N	3.7
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N	3.7
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N	3.7
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N	3.7
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N	3.7

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-34969

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-34969

Vulnerability Description

D-Bus before 1.15.6 sometimes allows unprivileged users to crash dbus-daemon. If a privileged user with control over the dbus-daemon is using the org.freedesktop.DBus.Monitoring interface to monitor message bus traffic, then an unprivileged user with the ability to connect to the same dbus-daemon can cause a dbus-daemon crash under some circumstances via an unreplyable message. When done on the well-known system bus, this is a denial-of-service vulnerability. The fixed versions are 1.12.28, 1.14.8, and 1.15.6.

CWE: CWE-617: Reachable Assertion

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2022-42010

Details

https://nvd.nist.gov/vuln/detail/CVE-2022-42010

Vulnerability Description

An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash when receiving a message with certain invalid type signatures.

CWE: CWE-347: Improper Verification of Cryptographic Signature

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2022-42011

Details

https://nvd.nist.gov/vuln/detail/CVE-2022-42011

Vulnerability Description

An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash when receiving a message where an array length is inconsistent with the size of the element type.

CWE: CWE-129: Improper Validation of Array Index

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2022-42012

Details

https://nvd.nist.gov/vuln/detail/CVE-2022-42012

Vulnerability Description

An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash by sending a message with attached file descriptors in an unexpected format.

CWE: CWE-400: Uncontrolled Resource Consumption

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2022-48554

Details

https://nvd.nist.gov/vuln/detail/CVE-2022-48554

Vulnerability Description

File before 5.43 has an stack-based buffer over-read in file_copystr in funcs.c. NOTE: "File" is the name of an Open Source project.

CWE: CWE-125: Out-of-bounds Read

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-29499

Summary

Gvariant offset table entry size is not checked in is_normal()

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-29499

Vulnerability Description

A flaw was found in GLib. GVariant deserialization fails to validate that the input conforms to the expected format, leading to denial of service.

CWE: CWE-400: Uncontrolled Resource Consumption

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-32636

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-32636

Vulnerability Description

A flaw was found in glib, where the gvariant deserialization code is vulnerable to a denial of service introduced by additional input validation added to resolve CVE-2023-29499. The offset table validation may be very slow. This bug does not affect any released version of glib but does affect glib distributors who followed the guidance of glib developers to backport the initial fix for CVE-2023-29499.

CWE: CWE-400: Uncontrolled Resource Consumption

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H	4.7
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H	4.7
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H	4.7
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H	4.7
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H	4.7
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H	4.7
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H	4.7
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H	4.7

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-32643

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-32643

Vulnerability Description

A flaw was found in GLib. The GVariant deserialization code is vulnerable to a heap buffer overflow introduced by the fix for CVE-2023-32665. This bug does not affect any released version of GLib, but does affect GLib distributors who followed the guidance of GLib developers to backport the initial fix for CVE-2023-32665.

CWE: CWE-122: Heap-based Buffer Overflow

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L	5.3
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L	5.3
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L	5.3
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L	5.3
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L	5.3
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L	5.3
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L	5.3
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L	5.3

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-32611

Summary

G_variant_byteswap() can take a long time with some non-normal inputs

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-32611

Vulnerability Description

A flaw was found in GLib. GVariant deserialization is vulnerable to a slowdown issue where a crafted GVariant can cause excessive processing, leading to denial of service.

CWE: CWE-400: Uncontrolled Resource Consumption

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-32665

Summary

Gvariant deserialisation does not match spec for non-normal data

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-32665

Vulnerability Description

A flaw was found in GLib. GVariant deserialization is vulnerable to an exponential blowup issue where a crafted GVariant can cause excessive processing, leading to denial of service.

CWE: CWE-400: Uncontrolled Resource Consumption

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-5156

Summary

Glibc: dos due to memory leak in getaddrinfo.c

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-5156

Vulnerability Description

A flaw was found in the GNU C Library. A recent fix for CVE-2023-4806 introduced the potential for a memory leak, which may result in an application crash.

CWE:	CWE-401: Missing Release of Memory after Effective Lifetime

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4911

Summary

Glibc: buffer overflow in ld.so leading to privilege escalation

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4911

Vulnerability Description

A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment variables when launching binaries with SUID permission to execute code with elevated privileges.

CWE: CWE-122: Heap-based Buffer Overflow

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2024-0553

Summary

Gnutls: incomplete fix for cve-2023-5981

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-0553

Vulnerability Description

A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from the response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the leakage of sensitive data. CVE-2024-0553 is designated as an incomplete resolution for CVE-2023-5981.

CWE: CWE-203: Observable Discrepancy

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2024-0567

Summary

Gnutls: rejects certificate chain with distributed trust

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-0567

Vulnerability Description

A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTLS) rejects a certificate chain with distributed trust. This issue occurs when validating a certificate chain with cockpit-certificate-ensure. This flaw allows an unauthenticated, remote client or attacker to initiate a denial of service attack.

CWE: CWE-347: Improper Verification of Cryptographic Signature

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-33953

Summary

Denial-of-Service in gRPC

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-33953

Vulnerability 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…

CWE: CWE-834: Excessive Iteration

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-32731

Summary

Information leak in gRPC

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-32731

Vulnerability Description

When gRPC HTTP2 stack raised a header size exceeded error, it skipped parsing the rest of the HPACK frame. This caused any HPACK table mutations to also be skipped, resulting in a desynchronization of HPACK tables between sender and receiver. If leveraged, say, between a proxy and a backend, this could lead to requests from the proxy being interpreted as containing headers from different proxy clients - leading to an information leak that can be used for privilege escalation or data exfiltration. We recommend upgrading beyond the commit contained in https://github.com/grpc/grpc/pull/33005 https://github.com/grpc/grpc/pull/33005

CWE: CWE-440: Expected Behavior Violation

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H	7.4
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H	7.4
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H	7.4
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H	7.4
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H	7.4
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H	7.4
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H	7.4
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H	7.4

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-32732

Summary

Denial-of-Service in gRPC

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-32732

Vulnerability 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

CWE: CWE-440: Expected Behavior Violation

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4785

Summary

Denial of Service in gRPC Core

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4785

Vulnerability 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.

CWE:	CWE-248: Uncaught Exception

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-44487

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-44487

Vulnerability 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.

CWE: CWE-400: Uncontrolled Resource Consumption

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-2603

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-2603

Vulnerability Description

A vulnerability was found in libcap. This issue occurs in the _libcap_strdup() function and can lead to an integer overflow if the input string is close to 4GiB.

CWE: CWE-190: Integer Overflow or Wraparound

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-6004

Summary

Libssh: proxycommand/proxyjump features allow injection of malicious code through hostname

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-6004

Vulnerability Description

A flaw was found in libssh. By utilizing the ProxyCommand or ProxyJump feature, users can exploit unchecked hostname syntax on the client. This issue may allow an attacker to inject malicious code into the command of the features mentioned through the hostname parameter.

CWE: CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-26551

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-26551

Vulnerability Description

mstolfp in libntp/mstolfp.c in NTP 4.2.8p15 has an out-of-bounds write in the cp<cpdec while loop. An adversary may be able to attack a client ntpq process, but cannot attack ntpd.

CWE: CWE-787: Out-of-bounds Write

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-26552

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-26552

Vulnerability Description

mstolfp in libntp/mstolfp.c in NTP 4.2.8p15 has an out-of-bounds write when adding a decimal point. An adversary may be able to attack a client ntpq process, but cannot attack ntpd.

CWE: CWE-787: Out-of-bounds Write

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-26553

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-26553

Vulnerability Description

mstolfp in libntp/mstolfp.c in NTP 4.2.8p15 has an out-of-bounds write when copying the trailing number. An adversary may be able to attack a client ntpq process, but cannot attack ntpd.

CWE: CWE-787: Out-of-bounds Write

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-26554

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-26554

Vulnerability Description

mstolfp in libntp/mstolfp.c in NTP 4.2.8p15 has an out-of-bounds write when adding a '\0' character. An adversary may be able to attack a client ntpq process, but cannot attack ntpd.

CWE: CWE-787: Out-of-bounds Write

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.6

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-26555

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-26555

Vulnerability Description

praecis_parse in ntpd/refclock_palisade.c in NTP 4.2.8p15 has an out-of-bounds write. Any attack method would be complex, e.g., with a manipulated GPS receiver.

CWE: CWE-787: Out-of-bounds Write

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	6.4
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	6.4
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	6.4
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	6.4
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	6.4
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	6.4
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	6.4
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	6.4

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2022-29900

Details

https://nvd.nist.gov/vuln/detail/CVE-2022-29900

Vulnerability Description

Mis-trained branch predictions for return instructions may allow arbitrary speculative code execution under certain microarchitecture-dependent conditions.

CWE: CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	6.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	6.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	6.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	6.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	6.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	6.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2022-29901

Summary

Arbitrary Memory Disclosure through CPU Side-Channel Attacks (Retbleed)

Details

https://nvd.nist.gov/vuln/detail/CVE-2022-29901

Vulnerability Description

Intel microprocessor generations 6 to 8 are affected by a new Spectre variant that is able to bypass their retpoline mitigation in the kernel to leak arbitrary data. An attacker with unprivileged user access can hijack return instructions to achieve arbitrary speculative code execution under certain microarchitecture-dependent conditions.

CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.6
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.6
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.6
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.6
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.6
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.6
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.6
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.6

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-48795

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-48795

Vulnerability Description

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

CWE: CWE-354: Improper Validation of Integrity Check Value

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-51384

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-51384

Vulnerability Description

In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.

CWE: CWE-304: Missing Critical Step in Authentication

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	5.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	5.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	5.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	5.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	5.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	5.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	5.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	5.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-51385

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-51385

Vulnerability Description

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.

CWE: CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-5363

Summary

Incorrect cipher key & IV length processing

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-5363

Vulnerability Description

Issue summary: A bug has been identified in the processing of key and initialisation vector (IV) lengths. This can lead to potential truncation or overruns during the initialisation of some symmetric ciphers.

Impact summary: A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes.

When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed after the key and IV have been established. Any alterations to the key length, via the "keylen" parameter or the IV length, via the "ivlen" parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB.

For the CCM, GCM and OCB cipher modes, truncation of the IV can result in loss of confidentiality. For example, when following NIST's SP 800-38D section 8.2.1 guidance for constructing a deterministic IV for AES in GCM mode, truncation of the counter portion could lead to IV reuse.

Both truncations and overruns of the key and overruns of the IV will produce incorrect results and could, in some cases, trigger a memory exception. However, these issues are not currently assessed as security critical.

Changing the key and/or IV lengths is not considered to be a common operation and the vulnerable API was recently introduced. Furthermore it is likely that application developers will have spotted this problem during testing since decryption would fail unless both peers in the communication were similarly vulnerable. For these reasons we expect the probability of an application being vulnerable to this to be quite low. However if an application is vulnerable then this issue is considered very serious. For these reasons we have assessed this issue as Moderate severity overall.

The OpenSSL SSL/TLS implementation is not affected by this issue.

The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this because the issue lies outside of the FIPS provider boundary.

OpenSSL 3.1 and 3.0 are vulnerable to this issue.

CWE: CWE-684: Incorrect Provision of Specified Functionality

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.6 LTS installed on AXC F 3152		

Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4807

Summary

POLY1305 MAC implementation corrupts XMM registers on Windows

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4807

Vulnerability Description

Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on the Windows 64 platform when running on newer X86_64 processors supporting the AVX512-IFMA instructions.

Impact summary: If in an application that uses the OpenSSL library an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences.

The POLY1305 MAC (message authentication code) implementation in OpenSSL does not save the contents of non-volatile XMM registers on Windows 64 platform when calculating the MAC of data larger than 64 bytes. Before returning to the caller all the XMM registers are set to zero rather than restoring

their previous content. The vulnerable code is used only on newer x86_64 processors supporting the AVX512-IFMA instructions.

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

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

As a workaround the AVX512-IFMA instructions support can be disabled at runtime by setting the environment variable OPENSSL_ia32cap:

OPENSSL_ia32cap=:~0x200000

The FIPS provider is not affected by this issue.

CWE: CWE-440: Expected Behavior Violation

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)

Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-3817

Summary

Excessive time spent checking DH q parameter value

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-3817

Vulnerability Description

Issue summary: Checking excessively long DH keys or parameters may be very slow.

Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.

The function DH_check() performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A correct q value, if present, cannot be larger than the modulus p parameter, thus it is unnecessary to perform these checks if q is larger than p.

An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack.

The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check().

Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the "-check" option.

The OpenSSL SSL/TLS implementation is not affected by this issue.

The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

CWE:	CWE-606: Unchecked Input for Loop Condition

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-47100

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-47100

Vulnerability Description

In Perl before 5.38.2, S_parse_uniprop_string in regcomp.c can write to unallocated space because a property name associated with a \p{...} regular expression construct is mishandled. The earliest affected version is 5.30.0.

CWE: CWE-755: Improper Handling of Exceptional Conditions

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2022-40897

Details

https://nvd.nist.gov/vuln/detail/CVE-2022-40897

Vulnerability 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.

CWE: CWE-1333: Inefficient Regular Expression Complexity

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-40217

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-40217

Vulnerability Description

An issue was discovered in Python before 3.8.18, 3.9.x before 3.9.18, 3.10.x before 3.10.13, and 3.11.x before 3.11.5. It primarily affects servers (such as HTTP servers) that use TLS client authentication. If a TLS server-side socket is created, receives data into the socket buffer, and then is closed quickly, there

is a brief window where the SSLSocket instance will detect the socket as "not connected" and won't initiate a handshake, but buffered data will still be readable from the socket buffer. This data will not be authenticated if the server-side TLS peer is expecting client certificate authentication, and is indistinguishable from valid TLS stream data. Data is limited in size to the amount that will fit in the buffer. (The TLS connection cannot directly be used for data exfiltration because the vulnerable code path requires that the connection be closed on initialization of the SSLSocket.)

CWE: CWE-305: Authentication Bypass by Primary Weakness

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4016

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4016

Vulnerability Description

Under some circumstances, this weakness allows a user who has access to run the “ps” utility on a machine, the ability to write almost unlimited amounts of unfiltered data into the process heap.

CWE: CWE-122: Heap-based Buffer Overflow

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L	2.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L	2.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L	2.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L	2.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L	2.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L	2.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L	2.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L	2.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-7104

Summary

SQLite SQLite3 make alltest sqlite3session.c sessionReadRecord heap-based overflow

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-7104

Vulnerability Description

A vulnerability was found in SQLite SQLite3 up to 3.43.0 and classified as critical. This issue affects the function sessionReadRecord of the file ext/session/sqlite3session.c of the component make alltest Handler. The manipulation leads to heap-based buffer overflow. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-248999.

CWE: CWE-122: Heap-based Buffer Overflow

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L	5.5
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L	5.5
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L	5.5
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L	5.5
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L	5.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L	5.5
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L	5.5
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L	5.5

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522

Order number: 1264328 (Download)

CVE-2021-41072

Details

https://nvd.nist.gov/vuln/detail/CVE-2021-41072

Vulnerability Description

squashfs_opendir in unsquash-2.c in Squashfs-Tools 4.5 allows Directory Traversal, a different vulnerability than CVE-2021-40153. A squashfs filesystem that has been crafted to include a symbolic link and then contents under the same filename in a filesystem can cause unsquashfs to first create the symbolic link pointing outside the expected directory, and then the subsequent write operation will cause the unsquashfs process to write through the symbolic link elsewhere in the filesystem.

CWE: CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H	8.1
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H	8.1
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H	8.1
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H	8.1
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H	8.1
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H	8.1
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H	8.1
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H	8.1

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R

Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-42465

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-42465

Vulnerability Description

Sudo before 1.9.15 might allow row hammer attacks (for authentication bypass or privilege escalation) because application logic sometimes is based on not equaling an error value (instead of equaling a success value), and because the values do not resist flips of a single bit.

CWE:	CWE-1319: Improper Protection against Electromagnetic Fault Injection (EM-FI)

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	7.0
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	7.0
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	7.0
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	7.0
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	7.0
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	7.0
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	7.0
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	7.0

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)

Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-5441

Summary

NULL Pointer Dereference in vim/vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-5441

Vulnerability Description

NULL Pointer Dereference in GitHub repository vim/vim prior to 20d161ace307e28690229b68584f2d84556f8960.

CWE:	CWE-476: NULL Pointer Dereference

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152

Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-5344

Summary

Heap-based Buffer Overflow in vim/vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-5344

Vulnerability Description

Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1969.

CWE: CWE-122: Heap-based Buffer Overflow

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)

Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-5535

Summary

Use After Free in vim/vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-5535

Vulnerability Description

Use After Free in GitHub repository vim/vim prior to v9.0.2010.

CWE:	CWE-416: Use After Free

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4781

Summary

Heap-based Buffer Overflow in vim/vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4781

Vulnerability Description

Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1873.

CWE: CWE-122: Heap-based Buffer Overflow

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8

Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4734

Summary

Integer Overflow or Wraparound in vim/vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4734

Vulnerability Description

Integer Overflow or Wraparound in GitHub repository vim/vim prior to 9.0.1846.

CWE:	CWE-190: Integer Overflow or Wraparound

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on BPC 9102S		

Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4733

Summary

Use After Free in vim/vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4733

Vulnerability Description

Use After Free in GitHub repository vim/vim prior to 9.0.1840.

CWE: CWE-416: Use After Free

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	7.3
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	7.3
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	7.3

Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	7.3
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	7.3
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	7.3
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	7.3
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	7.3

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4736

Summary

Untrusted Search Path in vim/vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4736

Vulnerability Description

Untrusted Search Path in GitHub repository vim/vim prior to 9.0.1833.

CWE: CWE-426: Untrusted Search Path

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8

Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4735

Summary

Out-of-bounds Write in vim/vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4735

Vulnerability Description

Out-of-bounds Write in GitHub repository vim/vim prior to 9.0.1847.

CWE:	CWE-787: Out-of-bounds Write

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L	4.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4750

Summary

Use After Free in vim/vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4750

Vulnerability Description

Use After Free in GitHub repository vim/vim prior to 9.0.1857.

CWE: CWE-416: Use After Free

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4738

Summary

Heap-based Buffer Overflow in vim/vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4738

Vulnerability Description

Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1848.

CWE: CWE-122: Heap-based Buffer Overflow

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4752

Summary

Use After Free in vim/vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4752

Vulnerability Description

Use After Free in GitHub repository vim/vim prior to 9.0.1858.

CWE: CWE-416: Use After Free

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-4751

Summary

Heap-based Buffer Overflow in vim/vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-4751

Vulnerability Description

Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1331.

CWE: CWE-122: Heap-based Buffer Overflow

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-48231

Summary

Use-After-Free in win_close() in vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-48231

Vulnerability Description

Vim is an open source command line text editor. When closing a window, vim may try to access already freed window structure. Exploitation beyond crashing the application has not been shown to be viable. This issue has been addressed in commit `25aabc2b` which has been included in release version 9.0.2106. Users are advised to upgrade. There are no known workarounds for this vulnerability.

CWE: CWE-416: Use After Free

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L	3.9
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L	3.9
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L	3.9
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L	3.9
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L	3.9
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L	3.9
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L	3.9
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L	3.9

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)

Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-48237

Summary

overflow in shift_line in vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-48237

Vulnerability Description

Vim is an open source command line text editor. In affected versions when shifting lines in operator pending mode and using a very large value, it may be possible to overflow the size of integer. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `6bf131888` which has been included in version 9.0.2112. Users are advised to upgrade. There are no known workarounds for this vulnerability.

CWE:	CWE-190: Integer Overflow or Wraparound

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L	2.8
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L	2.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L	2.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L	2.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L	2.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L	2.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L	2.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L	2.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)

Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-48706

Summary

Vim has heap-use-after-free at /src/charset.c:1770:12 in skipwhite

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-48706

Vulnerability Description

Vim is a UNIX editor that, prior to version 9.0.2121, has a heap-use-after-free vulnerability. When executing a :s command for the very first time and using a sub-replace-special atom inside the substitution part, it is possible that the recursive :s call causes free-ing of memory which may later then be accessed by the initial :s command. The user must intentionally execute the payload and the whole process is a bit tricky to do since it seems to work only reliably for the very first :s command. It may also cause a crash of Vim. Version 9.0.2121 contains a fix for this issue.

CWE:	CWE-416: Use After Free

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:L	3.6
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:L	3.6
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:L	3.6
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:L	3.6
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:L	3.6
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:L	3.6
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:L	3.6

Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:L	3.6

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-46246

Summary

Integer Overflow in :history command in Vim

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-46246

Vulnerability Description

Vim is an improved version of the good old UNIX editor Vi. Heap-use-after-free in memory allocated in the function `ga_grow_inner` in in the file `src/alloc.c` at line 748, which is freed in the file `src/ex_docmd.c` in the function `do_cmdline` at line 1010 and then used again in `src/cmdhist.c` at line 759. When using the `:history` command, it's possible that the provided argument overflows the accepted value. Causing an Integer Overflow and potentially later an use-after-free. This vulnerability has been patched in version 9.0.2068.

CWE: CWE-416: Use After Free

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.6 LTS installed on AXC F 3152		

Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	4.0

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

CVE-2023-45853

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-45853

Vulnerability Description

MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_64 via a long filename, comment, or extra field. NOTE: MiniZip is not a supported part of the zlib product. NOTE: pyminizip through 0.2.6 is also vulnerable because it bundles an affected zlib version, and exposes the applicable MiniZip code through its compress API.

CWE: CWE-190: Integer Overflow or Wraparound

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8

Firmware < 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.3 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2024.0.3 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 2024.0.6 LTS installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2024.0.6 LTS installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2024.0.6 LTS installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2024.0.6 LTS installed on BPC 9102S Order number: 1246285 (Download)
Firmware 2024.0.6 LTS installed on RFC 4072R Order number: 1136419 (Download)
Firmware 2024.0.3 LTS installed on EPC 1502 Order number: 1185416 (Download)
Firmware 2024.0.3 LTS installed on EPC 1522 Order number: 1264328 (Download)

Acknowledgments

Phoenix Contact GmbH & Co. KG thanks the following parties for their efforts:

- CERT@VDE for coordination. (see: https://certvde.com)

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

https://phoenixcontact.com/psirt

References

- PCSA-2024/00017 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- Phoenix Contact application note (EXTERNAL): https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf
-

- VDE-2024-073: Phoenix Contact: Multiple Vulnerabilities in PLCnext Firmware - HTML (SELF): https://certvde.com/en/advisories/VDE-2024-073
- VDE-2024-073: Phoenix Contact: Multiple Vulnerabilities in PLCnext Firmware - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2024/vde-2024-073.json

Revision history

Version	Date of the revision	Summary of the revision
1	Mon Dec 09 12:00:00 CET 2024	Initial

Sharing rules

TLP:WHITE

For the TLP version see https://www.first.org/tlp/