TLP:WHITE

VDE-2025-053: Phoenix Contact: Multiple Vulnerabilities in PLCnext Firmware

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue Jul 08 12:00:00 CEST 2025	Engine: 2.5.26
Current release date: Tue Jul 08 12:00:00 CEST 2025	Build Date: Wed May 28 16:30:36 CEST 2025
Current version: 1	Status: FINAL
CVSSv3.1 Base Score: 9.8	Severity: Critical
Original language: en	Language: en-GB
Also referred to: VDE-2025-053, PCSA-2025/00008	

Summary

Multiple Linux component vulnerabilities fixed in latest PLCnext Firmware release 2025.0.2

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 2025.0.2 Firmware Release. PHOENIX CONTACT recommends to always use an up-to-date version of the PLCnext Engineer.

Product groups

Affected Products.

- Firmware < 2025.0.2 installed on AXC F 1152
- Firmware < 2025.0.2 installed on AXC F 2152
- Firmware < 2025.0.2 installed on AXC F 3152
- Firmware < 2025.0.2 installed on RFC 4072S
- Firmware < 2025.0.2 installed on BPC 9102S

Fixed Product.

- Firmware 2025.0.2 installed on AXC F 1152
- Firmware 2025.0.2 installed on AXC F 2152
- Firmware 2025.0.2 installed on AXC F 3152
- Firmware 2025.0.2 installed on RFC 4072S
- Firmware 2025.0.2 installed on BPC 9102S

Vulnerabilities

CVE-2024-12705

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-12705

Vulnerability Description

Clients using DNS-over-HTTPS (DoH) can exhaust a DNS resolver's CPU and/or memory by flooding it with crafted valid or invalid HTTP/2 traffic. This issue affects BIND 9 versions 9.18.0 through 9.18.32, 9.20.0 through 9.20.4, 9.21.0 through 9.21.3, and 9.18.11-S1 through 9.18.32-S1.

CWE: CWE-770: Allocation of Resources Without Limits or Throttling

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2025-24965

Details

https://nvd.nist.gov/vuln/detail/CVE-2025-24965

Vulnerability Description

crun is an open source OCI Container Runtime fully written in C. In affected versions A malicious container image could trick the krun handler into escaping the root filesystem, allowing file creation or modification on the host. No special permissions are needed, only the ability for the current user to write to the target file. The problem is fixed in crun 1.20 and all users are advised to upgrade. There are no known workarounds for this vulnerability.

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 < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N	8.7
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N	8.7
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N	8.7
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N	8.7
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N	8.7

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2025-0665

Details

https://nvd.nist.gov/vuln/detail/CVE-2025-0665

Vulnerability Description

libcurl would wrongly close the same eventfd file descriptor twice when taking down a connection channel after having completed a threaded name resolve.

CWE: CWE-1341: Multiple Releases of Same Resource or Handle

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2025-0167

Details

https://nvd.nist.gov/vuln/detail/CVE-2025-0167

Vulnerability Description

When asked to use a `.netrc` file for credentials **and** to follow HTTP redirects, curl could leak the password used for the first host to the followed-to host under certain circumstances.

This flaw only manifests itself if the netrc file has a `default` entry that omits both login and password. A rare circumstance.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N	3.4
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N	3.4
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N	3.4
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N	3.4
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N	3.4

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-11053

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-11053

Vulnerability Description

When asked to both use a `.netrc` file for credentials and to follow HTTP redirects, curl could leak the password used for the first host to the followed-to host under certain circumstances.

This flaw only manifests itself if the netrc file has an entry that matches the redirect target hostname but the entry either omits just the password or omits both login and password.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N	3.4
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N	3.4
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N	3.4
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N	3.4
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N	3.4

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-9681

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-9681

Vulnerability Description

When curl is asked to use HSTS, the expiry time for a subdomain might overwrite a parent domain's cache entry, making it end sooner or later than otherwise intended.

This affects curl using applications that enable HSTS and use URLs with the insecure `HTTP://` scheme and perform transfers with hosts like `x.example.com` as well as `example.com` where the first host is a subdomain of the second host.

(The HSTS cache either needs to have been populated manually or there needs to have been previous HTTPS accesses done as the cache needs to have entries for the domains involved to trigger this problem.)

When `x.example.com` responds with `Strict-Transport-Security:` headers, this bug can make the subdomain's expiry timeout *bleed over* and get set for the parent domain `example.com` in curl's HSTS cache.

The result of a triggered bug is that HTTP accesses to `example.com` get converted to HTTPS for a different period of time than what was asked for by the origin server. If `example.com` for example stops supporting HTTPS at its expiry time, curl might then fail to access `http://example.com` until the (wrongly set) timeout expires. This bug can also expire the parent's entry *earlier*, thus making curl inadvertently switch back to insecure HTTP earlier than otherwise intended.

CWE: CWE-697: Incorrect Comparison

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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:L	6.5
Firmware < 2025.0.2 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:L	6.5
Firmware < 2025.0.2 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:L	6.5
Firmware < 2025.0.2 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:L	6.5
Firmware < 2025.0.2 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:L	6.5

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-0684

Coreutils: heap overflow in split --line-bytes with very long lines

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-0684

Vulnerability Description

A flaw was found in the GNU coreutils "split" program. A heap overflow with user-controlled data of multiple hundred bytes in length could occur in the line_bytes_split() function, potentially leading to an application crash and denial of service.

CWE: CWE-122: Heap-based Buffer Overflow

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	5.5
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	5.5
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	5.5
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	5.5
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	5.5

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-52533

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-52533

Vulnerability Description

gio/gsocks4aproxy.c in GNOME GLib before 2.82.1 has an off-by-one error and resultant buffer overflow because SOCKS4_CONN_MSG_LEN is not sufficient for a trailing '\0' character.

CWE: CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2020-16120

Unprivileged overlay + shiftfs read access

Details

https://nvd.nist.gov/vuln/detail/CVE-2020-16120

Vulnerability Description

Overlayfs did not properly perform permission checking when copying up files in an overlayfs and could be exploited from within a user namespace, if, for example, unprivileged user namespaces were allowed. It was possible to have a file not readable by an unprivileged user to be copied to a mountpoint controlled by the user, like a removable device. This was introduced in kernel version 4.19 by commit d1d04ef ("ovl: stack file ops"). This was fixed in kernel version 5.8 by commits 56230d9 ("ovl: verify permissions in ovl_path_open()"), 48bd024 ("ovl: switch to mounter creds in readdir") and 05acefb ("ovl: check permission to open real file"). Additionally, commits 130fdbc ("ovl: pass correct flags for opening real directory") and 292f902 ("ovl: call secutiry hook in ovl_real_ioctl()") in kernel 5.8 might also be desired or necessary. These additional commits introduced a regression in overlay mounts within user namespaces which prevented access to files with ownership outside of the user namespace. This regression was mitigated by subsequent commit b6650da ("ovl: do not fail because of O_NOATIMEi") in kernel 5.11.

CWE: CWE-266: Incorrect Privilege Assignment

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	5.1
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	5.1
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	5.1
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	5.1
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	5.1

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2023-7256

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-7256

Vulnerability Description

In affected libpcap versions during the setup of a remote packet capture the internal function sock_initaddress() calls getaddrinfo() and possibly freeaddrinfo(), but does not clearly indicate to the caller function whether freeaddrinfo() still remains to be called after the function returns. This makes it possible in some scenarios that both the function and its caller call freeaddrinfo() for the same allocated memory block. A similar problem was reported in Apple libpcap, to which Apple assigned CVE-2023-40400.

CWE: CWE-415: Double Free

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H	4.4
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H	4.4
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H	4.4
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H	4.4
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H	4.4

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-8006

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-8006

Vulnerability Description

Remote packet capture support is disabled by default in libpcap. When a user builds libpcap with remote packet capture support enabled, one of the functions that become available is pcap_findalldevs_ex(). One of the function arguments can be a filesystem path, which normally means a directory with input data files. When the specified path cannot be used as a directory, the function receives NULL from opendir(), but does not check the return value and passes the NULL value to readdir(), which causes a NULL pointer derefence.

CWE: CWE-476: NULL Pointer Dereference

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H	4.4
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H	4.4
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H	4.4
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H	4.4
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H	4.4

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-8176

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-8176

Vulnerability Description

A stack overflow vulnerability exists in the libexpat library due to the way it handles recursive entity expansion in XML documents. When parsing an XML document with deeply nested entity references, libexpat can be forced to recurse indefinitely, exhausting the stack space and causing a crash. This issue could lead to denial of service (DoS) or, in some cases, exploitable memory corruption, depending on the environment and library usage.

CWE: CWE-674: Uncontrolled Recursion

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-50602

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-50602

Vulnerability Description

An issue was discovered in libexpat before 2.6.4. There is a crash within the XML_ResumeParser function because XML_StopParser can stop/suspend an unstarted parser.

CWE: CWE-754: Improper Check for Unusual or Exceptional Conditions

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-10918

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-10918

Vulnerability Description

Stack-based Buffer Overflow vulnerability in libmodbus v3.1.10 allows to overflow the buffer allocated for the Modbus response if the function tries to reply to a Modbus request with an unexpected length.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-12133

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-12133

Vulnerability Description

A flaw in libtasn1 causes inefficient handling of specific certificate data. When processing a large number of elements in a certificate, libtasn1 takes much longer than expected, which can slow down or even crash the system. This flaw allows an attacker to send a specially crafted certificate, causing a denial of service attack.

CWE: CWE-407: Inefficient Algorithmic Complexity

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2025-27113

Details

https://nvd.nist.gov/vuln/detail/CVE-2025-27113

Vulnerability Description

libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a NULL pointer dereference in xmlPatMatch in pattern.c.

CWE: CWE-476: NULL Pointer Dereference

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-25062

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-25062

Vulnerability Description

An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.12.5. When using the XML Reader interface with DTD validation and XInclude expansion enabled, processing crafted XML documents can lead to an xmlValidatePopElement use-after-free.

CWE: CWE-416: Use After Free

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-5742

Nano: running `chmod` and `chown` on the filename allows malicious user to replace the emergency file with a malicious symlink to a root-owned file

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-5742

Vulnerability Description

A vulnerability was found in GNU Nano that allows a possible privilege escalation through an insecure temporary file. If Nano is killed while editing, a file it saves to an emergency file with the permissions of the running user provides a window of opportunity for attackers to escalate privileges through a malicious symlink.

CWE:	CWE-377: Insecure Temporary File

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N	4.7
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N	4.7
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N	4.7
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N	4.7
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N	4.7

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2025-26466

Details

https://nvd.nist.gov/vuln/detail/CVE-2025-26466

Vulnerability Description

A flaw was found in the OpenSSH package. For each ping packet the SSH server receives, a pong packet is allocated in a memory buffer and stored in a queue of packages. It is only freed when the server /client key exchange has finished. A malicious client may keep sending such packages, leading to an uncontrolled increase in memory consumption on the server side. Consequently, the server may become unavailable, resulting in a denial of service attack.

CWE: CWE-770: Allocation of Resources Without Limits or Throttling

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2025-26465

Details

https://nvd.nist.gov/vuln/detail/CVE-2025-26465

Vulnerability Description

A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can be performed by a malicious machine impersonating a legit server. This issue occurs due to how OpenSSH mishandles error codes in specific conditions when verifying the host key. For an attack to be considered successful, the attacker needs to manage to exhaust the client's memory resource first, turning the attack complexity high.

CWE: CWE-390: Detection of Error Condition Without Action

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N	6.8
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N	6.8
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N	6.8
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N	6.8
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N	6.8

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-6119

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-6119

Vulnerability Description

Issue summary: Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address resulting in abnormal termination of the application process.

Impact summary: Abnormal termination of an application can a cause a denial of service.

Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address when comparing the expected name with an `otherName` subject alternative name of an X.509 certificate. This may result in an exception that terminates the application program.

Note that basic certificate chain validation (signatures, dates, ...) is not affected, the denial of service can occur only when the application also specifies an expected DNS name, Email address or IP address.

TLS servers rarely solicit client certificates, and even when they do, they generally don't perform a name check against a reference identifier (expected identity), but rather extract the presented identity after checking the certificate chain. So TLS servers are generally not affected and the severity of the issue is Moderate.

The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.

CWE: CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-9143

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-9143

Vulnerability Description

Issue summary: Use of the low-level GF(2^m) elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes.

Impact summary: Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only "named curves" are supported, or, if explicit curve parameters are supported, they

specify an X9.62 encoding of binary (GF(2^m)) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low.

In particular, the X9.62 encoding is used for ECC keys in X.509 certificates, so problematic inputs cannot occur in the context of processing X.509 certificates. Any problematic use-cases would have to be using an "exotic" curve encoding.

The affected APIs include: EC_GROUP_new_curve_GF2m(), EC_GROUP_new_from_params(), and various supporting BN_GF2m_*() functions.

Applications working with "exotic" explicit binary (GF(2^m)) curve parameters, that make it possible to represent invalid field polynomials with a zero constant term, via the above or similar APIs, may terminate abruptly as a result of reading or writing outside of array bounds. Remote code execution cannot easily be ruled out.

The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-5535

SSL_select_next_proto buffer overread

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-5535

Vulnerability Description

Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer.

Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash. In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application.

The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists).

This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client /client_len parameters, and has additionally failed to correctly handle a "no overlap" response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem.

In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur.

This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely.

The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.

Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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:H	9.1
Firmware < 2025.0.2 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:H	9.1
Firmware < 2025.0.2 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:H	9.1
Firmware < 2025.0.2 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:H	9.1
Firmware < 2025.0.2 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:H	9.1

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-28882

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-28882

Vulnerability Description

OpenVPN from 2.6.0 through 2.6.10 in a server role accepts multiple exit notifications from authenticated clients which will extend the validity of a closing session

CWE: CWE-772: Missing Release of Resource after Effective Lifetime

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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:L	4.3
Firmware < 2025.0.2 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:L	4.3
Firmware < 2025.0.2 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:L	4.3
Firmware < 2025.0.2 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:L	4.3
Firmware < 2025.0.2 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:L	4.3

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-5594

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-5594

Vulnerability Description

OpenVPN before 2.6.11 does not santize PUSH_REPLY messages properly which an attacker controlling the server can use to inject unexpected arbitrary data ending up in client logs.

CWE: CWE-1287: Improper Validation of Specified Type of Input

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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:N	9.1
Firmware < 2025.0.2 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:N	9.1
Firmware < 2025.0.2 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:N	9.1
Firmware < 2025.0.2 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:N	9.1
Firmware < 2025.0.2 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:N	9.1

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2019-20633

Details

https://nvd.nist.gov/vuln/detail/CVE-2019-20633

Vulnerability Description

GNU patch through 2.7.6 contains a free(p_line[p_end]) Double Free vulnerability in the function another_hunk in pch.c that can cause a denial of service via a crafted patch file. NOTE: this issue exists because of an incomplete fix for CVE-2018-6952.

CWE: CWE-415: Double Free

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2019-13638

Details

https://nvd.nist.gov/vuln/detail/CVE-2019-13638

Vulnerability Description

GNU patch through 2.7.6 is vulnerable to OS shell command injection that can be exploited by opening a crafted patch file that contains an ed style diff payload with shell metacharacters. The ed editor does not need to be present on the vulnerable system. This is different from CVE-2018-1000156.

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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2019-13636

Details

https://nvd.nist.gov/vuln/detail/CVE-2019-13636

Vulnerability Description

In GNU patch through 2.7.6, the following of symlinks is mishandled in certain cases other than input files. This affects inp.c and util.c.

CWE: CWE-59: Improper Link Resolution Before File Access ('Link Following')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	5.9

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2018-1000156

Details

https://nvd.nist.gov/vuln/detail/CVE-2018-1000156

Vulnerability Description

GNU Patch version 2.7.6 contains an input validation vulnerability when processing patch files, specifically the EDITOR_PROGRAM invocation (using ed) can result in code execution. This attack appear to be exploitable via a patch file processed via the patch utility. This is similar to FreeBSD's CVE-2015-1418 however although they share a common ancestry the code bases have diverged over time.

CWE: CWE-20: Improper Input Validation

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2018-20969

Details

https://nvd.nist.gov/vuln/detail/CVE-2018-20969

Vulnerability Description

do_ed_script in pch.c in GNU patch through 2.7.6 does not block strings beginning with a ! character. NOTE: this is the same commit as for CVE-2019-13638, but the ! syntax is specific to ed, and is unrelated to a shell metacharacter.

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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2018-6951

Details

https://nvd.nist.gov/vuln/detail/CVE-2018-6951

Vulnerability Description

An issue was discovered in GNU patch through 2.7.6. There is a segmentation fault, associated with a NULL pointer dereference, leading to a denial of service in the intuit_diff_type function in pch.c, aka a "mangled rename" issue.

CWE:	CWE-476: NULL Pointer Dereference

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2018-6952

Details

https://nvd.nist.gov/vuln/detail/CVE-2018-6952

Vulnerability Description

A double free exists in the another_hunk function in pch.c in GNU patch through 2.7.6.

CWE: CWE-415: Double Free

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-9341

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-9341

Vulnerability Description

A flaw was found in Go. When FIPS mode is enabled on a system, container runtimes may incorrectly handle certain file paths due to improper validation in the containers/common Go library. This flaw allows an attacker to exploit symbolic links and trick the system into mounting sensitive host directories inside a container. This issue also allows attackers to access critical host files, bypassing the intended isolation between containers and the host system.

CWE: CWE-59: Improper Link Resolution Before File Access ('Link Following')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N	8.2
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N	8.2
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N	8.2
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N	8.2
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N	8.2

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2023-27043

Details

https://nvd.nist.gov/vuln/detail/CVE-2023-27043

Vulnerability Description

The email module of Python through 3.11.3 incorrectly parses e-mail addresses that contain a special character. The wrong portion of an RFC2822 header is identified as the value of the addr-spec. In some applications, an attacker can bypass a protection mechanism in which application access is granted only after verifying receipt of e-mail to a specific domain (e.g., only @company.example.com addresses may be used for signup). This occurs in email/_parseaddr.py in recent versions of Python.

CWE: CWE-20: Improper Input Validation

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-9287

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-9287

Vulnerability Description

A vulnerability has been found in the CPython venv module and CLI where path names provided when creating a virtual environment were not quoted properly, allowing the creator to inject commands into virtual environment "activation" scripts (ie "source venv/bin/activate"). This means that attacker-controlled virtual environments are able to run commands when the virtual environment is activated. Virtual environments which are not created by an attacker or which aren't activated before being used (ie "./venv /bin/python") are not affected.

CWE: CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-6232

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-6232

Vulnerability Description

There is a MEDIUM severity vulnerability affecting CPython.

Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives.

CWE: CWE-1333: Inefficient Regular Expression Complexity

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-6345

Remote Code Execution in pypa/setuptools

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-6345

Vulnerability Description

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

CWE: CWE-94: Improper Control of Generation of Code ('Code Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-12084

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-12084

Vulnerability Description

A heap-based buffer overflow flaw was found in the rsync daemon. This issue is due to improper handling of attacker-controlled checksum lengths (s2length) in the code. When MAX_DIGEST_LEN exceeds the fixed SUM_LENGTH (16 bytes), an attacker can write out of bounds in the sum2 buffer.

CWE: CWE-122: Heap-based Buffer Overflow

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-12085

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-12085

Vulnerability Description

A flaw was found in rsync which could be triggered when rsync compares file checksums. This flaw allows an attacker to manipulate the checksum length (s2length) to cause a comparison between a checksum and uninitialized memory and leak one byte of uninitialized stack data at a time.

CWE: CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-12086

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-12086

Vulnerability Description

A flaw was found in rsync. It could allow a server to enumerate the contents of an arbitrary file from the client's machine. This issue occurs when files are being copied from a client to a server. During this process, the rsync server will send checksums of local data to the client to compare with in order to determine what data needs to be sent to the server. By sending specially constructed checksum values for arbitrary files, an attacker may be able to reconstruct the data of those files byte-by-byte based on the responses from the client.

CWE: CWE-390: Detection of Error Condition Without Action

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:N/A:N	6.1
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:N/A:N	6.1
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:N/A:N	6.1
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:N/A:N	6.1
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:N/A:N	6.1

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-12087

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-12087

Vulnerability Description

A path traversal vulnerability exists in rsync. It stems from behavior enabled by the `--inc-recursive` option, a default-enabled option for many client options and can be enabled by the server even if not explicitly enabled by the client. When using the `--inc-recursive` option, a lack of proper symlink verification coupled with deduplication checks occurring on a per-file-list basis could allow a server to write files outside of the client's intended destination directory. A malicious server could write malicious files to arbitrary locations named after valid directories/paths on the client.

CWE: CWE-35: Path Traversal: '.../...//'

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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:N	6.5
Firmware < 2025.0.2 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:N	6.5
Firmware < 2025.0.2 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:N	6.5
Firmware < 2025.0.2 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:N	6.5
Firmware < 2025.0.2 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:N	6.5

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-12088

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-12088

Vulnerability Description

A flaw was found in rsync. When using the `--safe-links` option, the rsync client fails to properly verify if a symbolic link destination sent from the server contains another symbolic link within it. This results in a path traversal vulnerability, which may lead to arbitrary file write outside the desired directory.

CWE: CWE-35: Path Traversal: '.../...//'

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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:N	6.5
Firmware < 2025.0.2 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:N	6.5
Firmware < 2025.0.2 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:N	6.5
Firmware < 2025.0.2 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:N	6.5
Firmware < 2025.0.2 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:N	6.5

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-12747

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-12747

Vulnerability Description

A flaw was found in rsync. This vulnerability arises from a race condition during rsync's handling of symbolic links. Rsync's default behavior when encountering symbolic links is to skip them. If an attacker replaced a regular file with a symbolic link at the right time, it was possible to bypass the default behavior and traverse symbolic links. Depending on the privileges of the rsync process, an attacker could leak sensitive information, potentially leading to privilege escalation.

CWE: CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2022-0530

Details

https://nvd.nist.gov/vuln/detail/CVE-2022-0530

Vulnerability Description

A flaw was found in Unzip. The vulnerability occurs during the conversion of a wide string to a local string that leads to a heap of out-of-bound write. This flaw allows an attacker to input a specially crafted zip file, leading to a crash or code execution.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2022-0529

Details

https://nvd.nist.gov/vuln/detail/CVE-2022-0529

Vulnerability Description

A flaw was found in Unzip. The vulnerability occurs during the conversion of a wide string to a local string that leads to a heap of out-of-bound write. This flaw allows an attacker to input a specially crafted zip file, leading to a crash or code execution.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2021-4217

Details

https://nvd.nist.gov/vuln/detail/CVE-2021-4217

Vulnerability Description

A flaw was found in unzip. The vulnerability occurs due to improper handling of Unicode strings, which can lead to a null pointer dereference. This flaw allows an attacker to input a specially crafted zip file, leading to a crash or code execution.

CWE:	CWE-476: NULL Pointer Dereference

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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:L	3.3
Firmware < 2025.0.2 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:L	3.3
Firmware < 2025.0.2 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:L	3.3
Firmware < 2025.0.2 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:L	3.3
Firmware < 2025.0.2 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:L	3.3

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2018-1000035

Details

https://nvd.nist.gov/vuln/detail/CVE-2018-1000035

Vulnerability Description

A heap-based buffer overflow exists in Info-Zip UnZip version <= 6.00 in the processing of password-protected archives that allows an attacker to perform a denial of service or to possibly achieve code execution.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2018-18384

Details

https://nvd.nist.gov/vuln/detail/CVE-2018-18384

Vulnerability Description

Info-ZIP UnZip 6.0 has a buffer overflow in list.c, when a ZIP archive has a crafted relationship between the compressed-size value and the uncompressed-size value, because a buffer size is 10 and is supposed to be 12.

CWE: CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	5.5

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2016-9844

Details

https://nvd.nist.gov/vuln/detail/CVE-2016-9844

Vulnerability Description

Buffer overflow in the zi_short function in zipinfo.c in Info-Zip UnZip 6.0 allows remote attackers to cause a denial of service (crash) via a large compression method value in the central directory file header.

CWE: CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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 < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2019-13232

Details

https://nvd.nist.gov/vuln/detail/CVE-2019-13232

Vulnerability Description

Info-ZIP UnZip 6.0 mishandles the overlapping of files inside a ZIP container, leading to denial of service (resource consumption), aka a "better zip bomb" issue.

CWE: CWE-400: Uncontrolled Resource Consumption

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L	3.3
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L	3.3
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L	3.3
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L	3.3
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L	3.3

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2015-7696

Details

https://nvd.nist.gov/vuln/detail/CVE-2015-7696

Vulnerability Description

Info-ZIP UnZip 6.0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly execute arbitrary code via a crafted password-protected ZIP archive, possibly related to an Extra-Field size value.

CWE: CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Product status

Known affected

Product
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2015-7697

Details

https://nvd.nist.gov/vuln/detail/CVE-2015-7697

Vulnerability Description

Info-ZIP UnZip 6.0 allows remote attackers to cause a denial of service (infinite loop) via empty bzip2 data in a ZIP archive.

CWE:	CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

Product status

Known affected

Product
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-38428

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-38428

Vulnerability Description

url.c in GNU Wget through 1.24.5 mishandles semicolons in the userinfo subcomponent of a URI, and thus there may be insecure behavior in which data that was supposed to be in the userinfo subcomponent is misinterpreted to be part of the host subcomponent.

CWE:	CWE-436: Interpretation Conflict

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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:N	9.1
Firmware < 2025.0.2 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:N	9.1
Firmware < 2025.0.2 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:N	9.1
Firmware < 2025.0.2 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:N	9.1
Firmware < 2025.0.2 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:N	9.1

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2024-10524

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-10524

Vulnerability Description

Applications that use Wget to access a remote resource using shorthand URLs and pass arbitrary user credentials in the URL are vulnerable. In these cases attackers can enter crafted credentials which will cause Wget to access an arbitrary host.

CWE: CWE-918: Server-Side Request Forgery (SSRF)

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L	6.5
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L	6.5
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L	6.5
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L	6.5
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L	6.5

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (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

psirt@phoenixcontact.com

References

- PCSA-2025/00008 (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-2025-053: Phoenix Contact: Multiple Vulnerabilities in PLCnext Firmware - HTML (SELF): https://certvde.com/en/advisories/VDE-2025-053
- VDE-2025-053: Phoenix Contact: Multiple Vulnerabilities in PLCnext Firmware - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2025/vde-2025-053.json

Revision history

Version	Date of the revision	Summary of the revision
1	Tue Jul 08 12:00:00 CEST 2025	Initial

Sharing rules

TLP:WHITE

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