TLP:WHITE

VDE-2024-071: 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: Mon Dec 02 17:25:30 CET 2024
Current version: 1	Status: FINAL
CVSSv3.1 Base Score: 9.0	Severity: Critical
Original language: en	Language: en-GB
Also referred to: VDE-2024-071, PCSA-2024/00016	

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. Check download area for latest Firmware update to be installed on EPC 1502 or EPC 1522.

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 < 2024.0.6 LTS installed on EPC 1502
- Firmware < 2024.0.6 LTS installed on EPC 1522

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

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

Vulnerabilities

CVE-2024-4741

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-4741

Vulnerability Description

A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications.

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: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 < 2024.0.6 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 < 2024.0.6 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

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

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)

CVE-2024-6387

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-6387

Vulnerability Description

A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

CWE: CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race 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:H/PR:N/UI:N/S:U/C:H/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:H/PR:N/UI:N/S:U/C:H/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:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1
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:H/A:H	8.1
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:H/A:H	8.1
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:H/A:H	8.1
Firmware < 2024.0.6 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1
Firmware < 2024.0.6 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

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)

CVE-2024-39894

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-39894

Vulnerability Description

OpenSSH 9.5 through 9.7 before 9.8 sometimes allows timing attacks against echo-off password entry (e.g., for su and Sudo) because of an ObscureKeystrokeTiming logic error. Similarly, other timing attacks against keystroke entry could occur.

CWE: CWE-367: Time-of-check Time-of-use (TOCTOU) Race 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:H/PR:N/UI:R/S:U/C:H/I:H/A:H	7.5
Firmware < 2024.0.6 LTS 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:H	7.5
Firmware < 2024.0.6 LTS 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:H	7.5
Firmware < 2024.0.6 LTS 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:H	7.5
Firmware < 2024.0.6 LTS 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:H	7.5
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H	7.5
Firmware < 2024.0.6 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H	7.5
Firmware < 2024.0.6 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H	7.5

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

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)

CVE-2024-32002

Summary

Git's recursive clones on case-insensitive filesystems that support symlinks are susceptible to Remote Code Execution

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-32002

Vulnerability Description

Git is a revision control system. Prior to versions 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2, and 2.39.4, repositories with submodules can be crafted in a way that exploits a bug in Git whereby it can be fooled into writing files not into the submodule's worktree but into a `.git/` directory. This allows writing a hook that will be executed while the clone operation is still running, giving the user no opportunity to inspect the code that is being executed. The problem has been patched in versions 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2, and 2.39.4. If symbolic link support is disabled in Git (e.g. via `git config --global core.symlinks false`), the described attack won't work. As always, it is best to avoid cloning repositories from untrusted sources.

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

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

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:C/C:H/I:H/A:H	9.0
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:C/C:H/I:H/A:H	9.0
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:C/C:H/I:H/A:H	9.0
Firmware < 2024.0.6 LTS installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	9.0
Firmware < 2024.0.6 LTS installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	9.0
Firmware < 2024.0.6 LTS installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	9.0
Firmware < 2024.0.6 LTS installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	9.0
Firmware < 2024.0.6 LTS installed on EPC 1522 Order number: 1264328	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	9.0

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)

CVE-2024-4603

Summary

Excessive time spent checking DSA keys and parameters

Details

https://nvd.nist.gov/vuln/detail/CVE-2024-4603

Vulnerability Description

Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary: Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA parameters may experience long delays. Where the key or parameters that are

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

being checked have been obtained from an untrusted source this may lead to a Denial of Service. The functions EVP_PKEY_param_check() or EVP_PKEY_public_check() perform various checks on DSA parameters. Some of those computations take a long time if the modulus (p parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls EVP_PKEY_param_check() or EVP_PKEY_public_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable. Also vulnerable are the OpenSSL pkey 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 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 < 2024.0.6 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 < 2024.0.6 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)

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

CVE-2024-2511

Summary

Unbounded memory growth with session handling in TLSv1.3

Details

https://www.suse.com/security/cve/CVE-2024-2511.html

Vulnerability Description

Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

CWE: CWE-1325: Improperly Controlled Sequential Memory Allocation

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 < 2024.0.6 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 < 2024.0.6 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

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

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)

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-2024/00016 (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-2024-071: Phoenix Contact: Multiple Vulnerabilities in PLCnext Firmware - HTML (SELF): https://certvde.com/en/advisories/VDE-2024-071
- VDE-2024-071: Phoenix Contact: Multiple Vulnerabilities in PLCnext Firmware - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2024/vde-2024-071.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/

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany