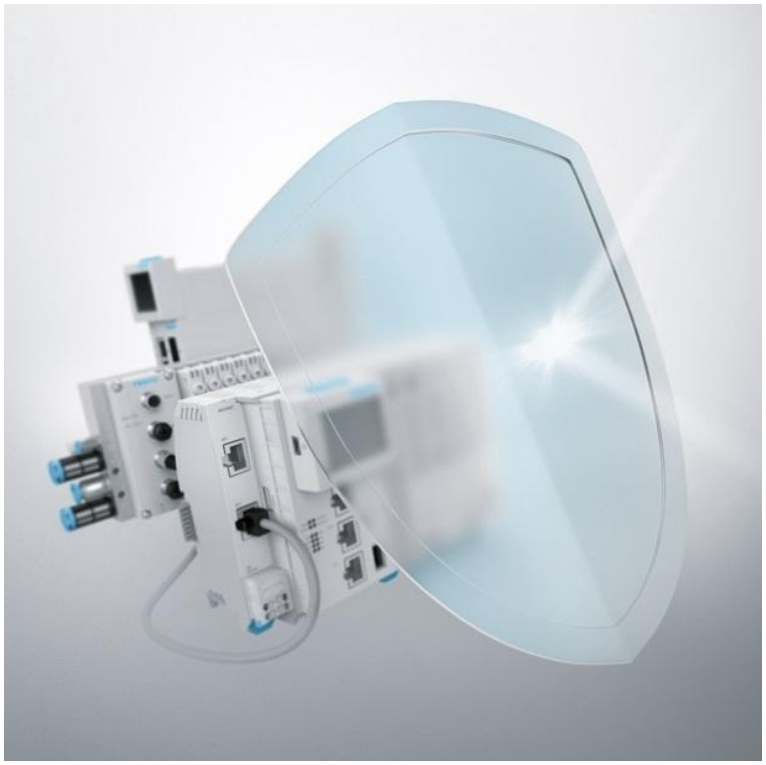
Multiple OpenSSL vulnerabilities affect Festo AX OS in CEPE



FSA-202602

Date
October 20th, 2026

Creator
Festo SE & Co. KG

Version
1.0.0

Festo SE & Co. KG

www.festo.com/psirt
psirt@festo.com
Ruiter Straße 82
73734 Esslingen
GERMANY

Summary

Festo AX OS versions 25.0.1.46 and 25.9.2.4, which are based on PLCnext by Phoenix Contact, used by the Festo product CEPE are affected by multiple OpenSSL vulnerabilities. The vulnerabilities are identified as CVE-2025-15467 and CVE-2025-69419. Attacks may be possible when maliciously crafted firmware, key files, PKCS#12 files, CMS/PKCS#7 content, or digitally signed objects are uploaded and processed by the affected system. In the device context, exploitation typically requires a logged-in user with high privileges or the processing of attacker-supplied cryptographic objects.

A successful attack using manipulated firmware, key files, PKCS#12 files, CMS/PKCS#7 content, or digitally signed objects may lead to memory corruption, application crash, or denial of service. Depending on the affected code path, execution context, platform protections, and toolchain mitigations, execution of malicious code may be possible. This can jeopardize confidentiality, integrity, and availability of the affected system.

Vulnerability Identifier

CVEs: CVE-2025-15467, CVE-2025-69419

Severity

9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected Vendors

Festo

Affected Products and Remediations

Affected Product and Versions	Product Details	Remediation
CEPE Firmware Festo AX OS: AX OS 25.0.1.46 affected		For CVE-2025-15467, CVE-2025-69419: Update affected CEPE installations running Festo AX OS 25.0.1.46 or Festo AX OS 25.9.2.4 to Festo AX OS 26.3.1.4 or later.
CEPE Firmware Festo AX OS:		For CVE-2025-15467, CVE-2025-69419: Update affected CEPE installations running Festo AX OS 25.0.1.46 or Festo AX OS 25.9.2.4 to Festo AX OS 26.3.1.4 or later.

Affected Product and Versions	Product Details	Remediation
AX OS 25.9.2.4 affected		

Workarounds and Mitigations

Remediations can be found in the table of Affected Products and Recommendations.

Additionally, please refer to the General Recommendations.

Impact and Classification of Vulnerabilities

CVE-2025-15467
Parsing CMS AuthEnvelopedData or EnvelopedData message with maliciously crafted AEAD parameters can trigger a stack buffer overflow.

CVSS v3.1 Base Score	9.8
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE	CWE-787: Out-of-bounds Write

CVE-2025-69419
Calling PKCS12_get_friendlyname() function on a maliciously crafted PKCS#12 file with a BMPString (UTF-16BE) friendly name containing non-ASCII BMP code point can trigger a one byte write before the allocated buffer.

CVSS v3.1 Base Score	7.4
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
CWE	CWE-787: Out-of-bounds Write

General recommendations

As part of a security strategy, Festo recommends the following general defense measures to reduce the risk of exploits:

- Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside.
- Use firewalls to protect and separate the control system network from other networks.
- Use VPN (Virtual Private Networks) tunnels if remote access is required.
- Activate and apply user management and password features.
- Use encrypted communication links.
- Limit the access to both development and control system by physical means, operating system features, etc.
- Protect both development and control systems by using up-to-date virus detection solutions.

Festo strongly recommends minimizing and protecting network access to connected devices with state-of-the-art techniques and processes.
To ensure secure operation follow the recommendations in the product manuals.

Acknowledgments

Festo SE & Co. KG thanks the following parties for their efforts:

- CERT@VDE for coordination and support with this publication

Publisher Details

https://www.festo.com
psirt@festo.com
For further security-related issues in Festo products please contact the Festo Product Security Incident Response Team (PSIRT) https://www.festo.com/psirt

Further References

For further information also refer to:

- CERT@VDE Advisory https://certvde.com/en/advisories/vendor/festo/

- Phoenix Contact Advisory PCSA-2026-00001 / VDE-2026-023: Several products are affected by vulnerabilities found in OpenSSL https://phoenixcontact.com/psirt
- FSA-202602: Multiple OpenSSL vulnerabilities affect Festo AX OS in CEPE - CSAF https://festo.csaf-tp.certvde.com/.well-known/csaf/white/2026/fsa-202602.json
- FSA-202602: Multiple OpenSSL vulnerabilities affect Festo AX OS in CEPE - HTML https://certvde.com/en/advisories/VDE-2026-090

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	October 20th, 2026	Initial Revision

Sharing rules

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

Disclaimer

Festo assumes no liability whatsoever for indirect, collateral, accidental or consequential losses that occur by the distribution and/or use of this document or any losses in connection with the distribution and/or use of this document. All information published in this document is provided free of charge and on good faith by Festo. Insofar as permissible by law, however, none of this information shall establish any warranty, guarantee, commitment, or liability on the part of Festo.

Note: In no case does this information release the operator or responsible person from the obligation to check the effect on his system or installation before using the information and, in the event of negative consequences, not to use the information.

In addition, the actual general terms, and conditions for delivery, payment and software use of Festo, available under http://www.festo.com and the special provisions for the use of Festo Security Advisory available at https://www.festo.com/psirt shall apply.