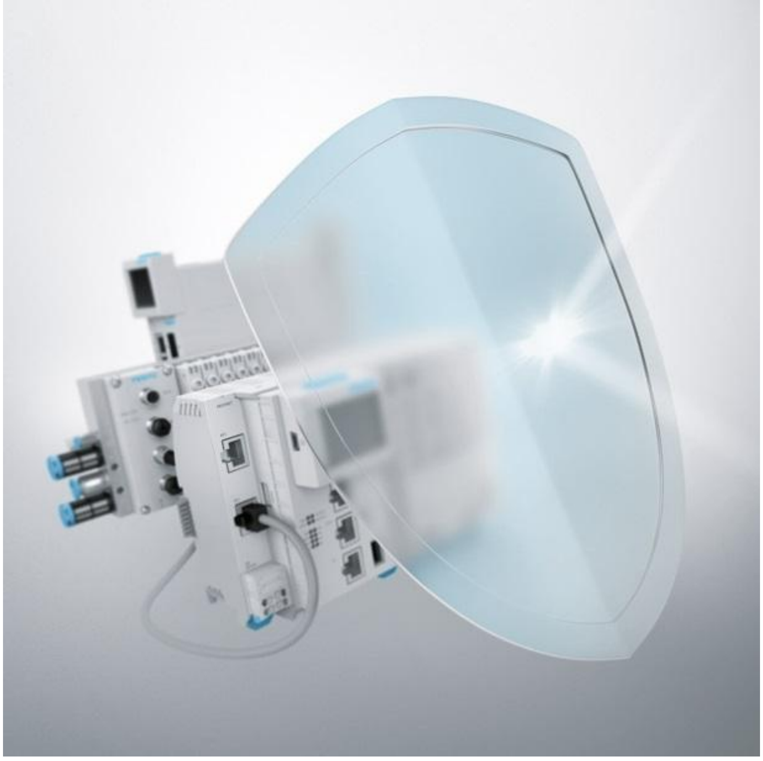
Festo Controller CECC-X-M1 Product Family - Pre-Authentication Command Injection Vulnerability



FSA-202201

Date
January 11th, 2024

Creator
Festo SE & Co. KG

Version
1.1.1

Festo SE & Co. KG

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

Summary

The Festo controller CECC-X-M1 product family in multiple versions are affected by a pre-authentication command injection vulnerability. Any person who is able to gain access to the webserver would be able to run arbitrary system commands on the device with root privileges.

Vulnerability Identifier

CVEs: CVE-2022-30308, CVE-2022-30309, CVE-2022-30310, CVE-2022-30311

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
Controller CECC-X-M1: Firmware CECC-X <= 3.8.14 affected	Festo:Partnumber:4407603 Festo:Ordercode:CECC-X-M1	For all vulnerability identifiers: Update to Firmware CECC-X 3.8.18 or later version.
Controller CECC-X-M1: Firmware CECC-X 4.0.14 affected	Festo:Partnumber:8124922 Festo:Ordercode:CECC-X-M1	For all vulnerability identifiers: Update to Firmware CECC-X 4.0.18 or later version.
Controller CECC-X-M1-MV: Firmware CECC-X <= 3.8.14 affected	Festo:Partnumber:4407605 Festo:Ordercode:CECC-X-M1-MV	For all vulnerability identifiers: Update to Firmware CECC-X 3.8.18 or later version.
Controller CECC-X-M1-MV: Firmware CECC-X 4.0.14 affected	Festo:Partnumber:8124923 Festo:Ordercode:CECC-X-M1-MV	For all vulnerability identifiers: Update to Firmware CECC-X 4.0.18 or later version.
Controller CECC-X-M1-MV-S1: Firmware CECC-X <= 3.8.14 affected	Festo:Partnumber:4407606 Festo:Ordercode:CECC-X-M1-MV-S1	For all vulnerability identifiers: Update to Firmware CECC-X 3.8.18 or later version.
Controller CECC-X-M1-MV-S1:		

Affected Product and Versions	Product Details	Remediation
Firmware CECC-X 4.0.14 affected	Festo:Partnumber:8124924 Festo:Ordercode:CECC-X-M1-MV-S1	For all vulnerability identifiers: Update to Firmware CECC-X 4.0.18 or later version.
Controller CECC-X-M1-Y-YJKP: Firmware CECC-X <= 3.8.14 affected	Festo:Partnumber:4803891 Festo:Ordercode:CECC-X-M1-Y-YJKP	For all vulnerability identifiers: Update to Firmware CECC-X 3.8.18 or later version.
Controller CECC-X-M1-YS-L1: Firmware CECC-X <= 3.8.14 affected	Festo:Partnumber:8082793 Festo:Ordercode:CECC-X-M1-YS-L1	For all vulnerability identifiers: Update to Firmware CECC-X 3.8.18 or later version.
Controller CECC-X-M1-YS-L2: Firmware CECC-X <= 3.8.14 affected	Festo:Partnumber:8082794 Festo:Ordercode:CECC-X-M1-YS-L2	For all vulnerability identifiers: Update to Firmware CECC-X 3.8.18 or later version.
Servo Press Kit YJKP: Firmware CECC-X <= 3.8.14 affected	Festo:Partnumber:8077950 Festo:Ordercode:YJKP	For all vulnerability identifiers: Update to Firmware CECC-X 3.8.18 or later version.
Servo Press Kit YJKP-: Firmware CECC-X <= 3.8.14 affected	Festo:Partnumber:8058596 Festo:Ordercode:YJKP-	For all vulnerability identifiers: Update to Firmware CECC-X 3.8.18 or later version.

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-2022-30308
In Festo Controller CECC-X-M1 product family, the http-endpoint “cecc-x-web-viewer-request-on” POST request doesn’t check for port syntax. This can result in unauthorized execution of system commands with root privileges due to improper access control command injection.
Weakness: Incorrect Authorization (CWE-863)

Base Score: 9.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2022-30309
In Festo Controller CECC-X-M1 product family, the http-endpoint “cecc-x-web-viewer-request-off” POST request doesn’t check for port syntax. This can result in unauthorized execution of system commands with root privileges due to improper access control command injection.
Weakness: Incorrect Authorization (CWE-863)
Base Score: 9.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2022-30310
In Festo Controller CECC-X-M1 product family, the http-endpoint “cecc-x-acknerr-request” POST request doesn’t check for port syntax. This can result in unauthorized execution of system commands with root privileges due to improper access control command injection.
Weakness: Incorrect Authorization (CWE-863)
Base Score: 9.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2022-30311
In Festo Controller CECC-X-M1 product family, the http-endpoint “cecc-x-refresh-request” POST request doesn’t check for port syntax. This can result in unauthorized execution of system commands with root privileges due to improper access control command injection.
Weakness: Incorrect Authorization (CWE-863)
Base Score: 9.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

General recommendations

Currently, Festo has not identified any specific workarounds for this vulnerability.

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 system by using up to date virus detecting solutions

Festo strongly recommends to minimize and protect network access to connected devices with state of the art techniques and processes.

For a 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 (see: https://cert.vde.com/)
- Q. Kaiser, M. Illes from ONEKEY Research Labs for reporting to Festo (see: https://onekey.com/)

Publisher Details

https://festo.com/
Festo SE & Co. KG, PSIRT, Ruiter Straße 82, 73734 Esslingen Germany, psirt@festo.com
For further security-related issues in Festo products please contact the Festo Product Security Incident Response Team (PSIRT): https://festo.com/psirt

Further References

For further information also refer to:

- VDE-2022-020
- CERT@VDE Security Advisories https://cert.vde.com/en/advisories/vendor/festo/

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	June 08th, 2022	Initial version
1.1.0	July 05th, 2022	Updated CWE on vulnerability description, added released firmware version fixing the issues.
1.1.1	January 11th, 2024	Adjust link to VDE Advisory

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 these 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 of Festo for delivery, payment and software use shall apply, available under http://www.festo.com.