

Forum:[Hack Forums](#)

Thread: [FESTO Hardware Controller, Hardware Servo Press Kit](#)

Stanley - July 16, 2025, 6:20 am

FESTO Hardware Controller, Hardware Servo Press Kit

View CSAF

1. EXECUTIVE SUMMARY

CVSS v3 9.8

ATTENTION: Exploitable remotely/low attack complexity

Vendor: FESTO

Equipment: Hardware Controller, Hardware Servo Press Kit

Vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to execute unauthorized system commands with root privileges.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

FESTO reports the following products are affected:

Festo Firmware installed on Festo Hardware Controller CECC-X-M1: Version 4.0.14

Festo Firmware installed on Festo Hardware Controller CECC-X-M1: Versions 3.8.14 and prior

Festo Firmware installed on Festo Hardware Controller CECC-X-M1-MV: Versions 3.8.14 and prior

Festo Firmware installed on Festo Hardware Controller CECC-X-M1-MV: Version 4.0.14

Festo Firmware installed on Festo Hardware Controller CECC-X-M1-MV-S1: Version 4.0.14

Festo Firmware installed on Festo Hardware Controller CECC-X-M1-MV-S1: Versions 3.8.14 and prior

Festo Firmware installed on Festo Hardware Controller CECC-X-M1-YS-L1: Versions 3.8.14 and prior

Festo Firmware installed on Festo Hardware Controller CECC-X-M1-YS-L2: Versions 3.8.14 and prior

Festo Firmware installed on Festo Hardware Controller CECC-X-M1-Y-YJKP: Versions 3.8.14 and prior

Festo Firmware installed on Festo Hardware Servo Press Kit YJKP: Versions 3.8.14 and prior

Festo Firmware installed on Festo Hardware Servo Press Kit YJKP-: Versions 3.8.14 and prior

3.2 VULNERABILITY OVERVIEW

3.2.1 IMPROPER NEUTRALIZATION OF SPECIAL ELEMENTS USED IN AN OS COMMAND ('OS COMMAND INJECTION') CWE-78

In multiple versions of 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.

CVE-2022-30311 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.8 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

3.2.2 IMPROPER NEUTRALIZATION OF SPECIAL ELEMENTS USED IN AN OS COMMAND ('OS

COMMAND INJECTION') CWE-78

In multiple versions of 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.

CVE-2022-30310 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.8 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

3.2.3 IMPROPER NEUTRALIZATION OF SPECIAL ELEMENTS USED IN AN OS COMMAND ('OS COMMAND INJECTION') CWE-78

In multiple versions of 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.

CVE-2022-30309 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.8 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

3.2.4 IMPROPER NEUTRALIZATION OF SPECIAL ELEMENTS USED IN AN OS COMMAND ('OS COMMAND INJECTION') CWE-78

In multiple versions of 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.

CVE-2022-30308 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.8 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

3.3 BACKGROUND

CRITICAL INFRASTRUCTURE SECTORS: Critical Manufacturing

COUNTRIES/AREAS DEPLOYED: Worldwide

COMPANY HEADQUARTERS LOCATION: Germany

3.4 RESEARCHER

Q. Kaiser and M. Illes of ONEKEY Research Labs reported these vulnerabilities to Festo. CERT@VDE coordinated with and supported Festo in the publication of FSA-202201.

4. MITIGATIONS

FESTO recommends users update to Firmware CECC-X 4.0.18 or later versions.

For more information see the associated Festo SE & Co. KG security advisory FSA-202201 VDE-2022-020: Festo: CECC-X-M1 - command injection vulnerabilities.

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities, such as:

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs). Recognize VPNs may have vulnerabilities, should be updated to the most recent version available, and are only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on [cisa.gov](https://www.cisa.gov). Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at [cisa.gov](https://www.cisa.gov) in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

Do not click web links or open attachments in unsolicited email messages.

Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.

Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

No known public exploitation specifically targeting these vulnerabilities has been reported to CISA at this time.

5. UPDATE HISTORY

July 1, 2025: Initial Republication of Festo SE & Co. KG FSA-202201

<https://www.cisa.gov/news-events/ics-advisories/icsa-25-182-04>