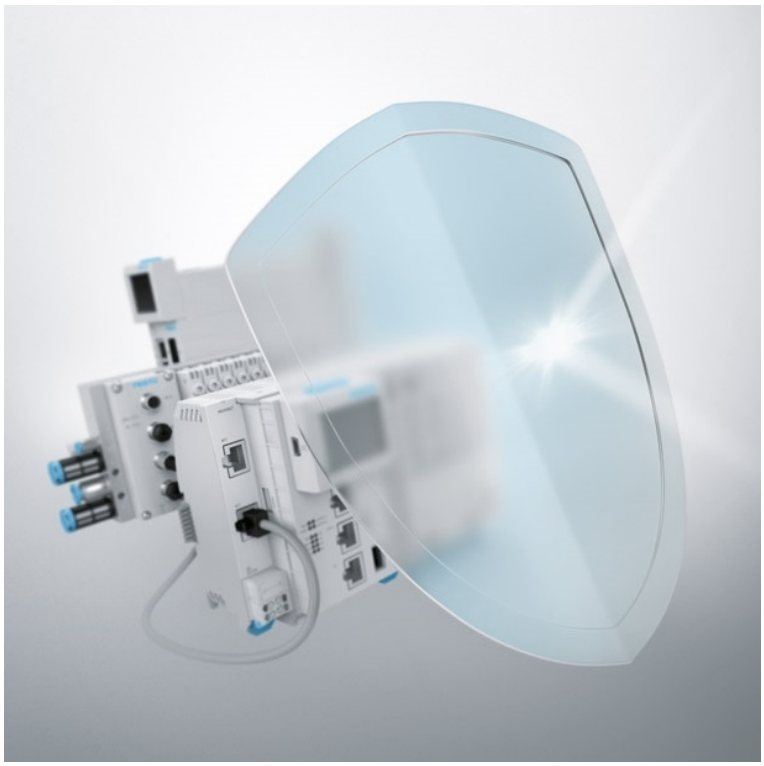
CPX-CEC-C1 and CPX-CMXX, Missing Authentication for Critical Webpage Function



FSA-202207

Date
October 18th, 2022

Creator
Festo SE & Co. KG

Version
1.1.0

Festo SE & Co. KG

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

Summary

Unauthenticated access to critical webpage functions (e.g. reboot) may cause a denial of service of the device.

Vulnerability Identifier

CVEs: CVE-2022-3079

Severity

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

Affected Vendors

FESTO

Affected Products and Remediations

Affected Product and Versions	Product Details	Remediation
Control block CPX-CEC-C1: CPX-CEC-C1 Hardware all versions: Control block CPX-CEC-C1 Firmware <= 2.0.12 affected	Festo:Partnumber: 567347 Festo:Ordercode:CPX-CEC-C1	For all vulnerability identifiers: Currently no fix is planned. Replace CPX-CEC-C1 with follow-up product CPX-CEC-C1-V3. For further mitigations see general recommendations. See section Workarounds and Mitigations.
Control block-SET CPX-CEC-C1: CPX-CEC-C1 Hardware all versions: Control block CPX-CEC-C1 Firmware <= 2.0.12 affected	Festo:Partnumber: 568714 Festo:Ordercode:CPX-CEC-C1	For all vulnerability identifiers: Currently no fix is planned. Replace CPX-CEC-C1 with follow-up product CPX-CEC-C1-V3. For further mitigations see general recommendations. See section Workarounds and Mitigations.

Affected Product and Versions	Product Details	Remediation
Control block CPX-CMXX: CPX-CMXX Hardware all versions: Control block CPX-CMXX Firmware <= 1.2.34 rev.404 affected	Festo:Partnumber: 555667 Festo:Ordercode:CPX-CMXX	For all vulnerability identifiers: Currently no fix is planned. Replace CPX-CMXX with follow up product CPX-CEC-M1-V3. For further mitigations see general recommendations. See section Workarounds and Mitigations.
Control block-SET CPX-CMXX: CPX-CMXX Hardware all versions: Control block CPX-CMXX Firmware <= 1.2.34 rev.404 affected	Festo:Partnumber: 555668 Festo:Ordercode:CPX-CMXX	For all vulnerability identifiers: Currently no fix is planned. Replace CPX-CMXX with follow up product CPX-CEC-M1-V3. For further mitigations see general recommendations. See section Workarounds and Mitigations.

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-2022-3079
Festo control block CPX-CEC-C1 and CPX-CMXX in multiple versions allow unauthenticated, remote access to critical webpage functions which may cause a denial of service.
Weakness: Improper Privilege Management (CWE-269)
Base Score: 7.5
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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 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/)
- Daniel dos Santos, Rob Hulsebos from Forescout for reporting to Festo (see: https://forescout.com/)

Publisher Details

https://festo.com/psirt

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

Also refer to:

- https://cert.vde.com/en/advisories/VDE-2022-036/
- CERT@VDE Security Advisories https://cert.vde.com/en/advisories/vendor/festo/
- CVE Entry at mitre https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3079

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	September 20th, 2022	intial release version
1.1.0	October 17th, 2022	Added the product SETs for both products

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.