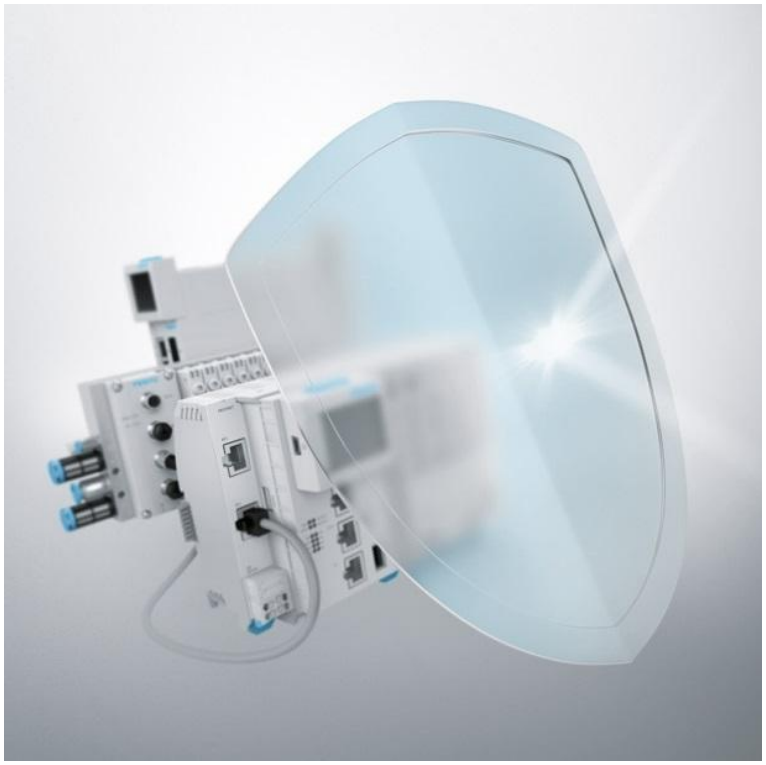
Multiple Festo products contain an unsafe default Codesys configuration



FSA-202208

Date
January 11th, 2024

Creator
Festo SE & Co. KG

Version
1.0.1

Festo SE & Co. KG

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

Summary

The products are shipped with an unsafe configuration of the integrated CODESYS Runtime environment. In this case no default password is set to the CODESYS PLC and therefore access without authentication is possible.

With a successful established connection to the CODESYS Runtime the PLC-Browser commands are available. Thus granting the possibilities to e.g. read and modify the configuration file(s), start/stop the application and reboot the device.

Vulnerability Identifier

CVEs: CVE-2022-22515, CVE-2022-31806

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
Operator unit CDPX: Operator unit CDPX all versions affected	Festo:Ordercode:CDPX-X-A-W-4, CDPX-X-A-W-7, CDPX-X-A-W-13, CDPX-X-A-S-10, CDPX-X-E1-W-7, CDPX-X-E1-W-10, CDPX-X-E1-W-15	For CVE-2022-22515: Currently no fix is planned. For further mitigations see general recommendations. See section Workarounds and Mitigations.
Controller CECC: Controller CECC all versions affected	Festo:Ordercode:CECC-D, CECC-D-BA, CECC-D-CS, CECC-LK, CECC-S, CECC-X-M1, CECC-X-M1-MV, CECC-X-M1-S1	For CVE-2022-22515: Currently no fix is planned. For further mitigations see general recommendations. See section Workarounds and Mitigations.
Controller CECX-X: Controller CECX-X	Festo:Partnumber:553852, 553853 Festo:Ordercode:CECX-X-C1, CECX-X-M1	For CVE-2022-31806: Currently no fix is planned. For further mitigations see general recommendations.

Affected Product and Versions	Product Details	Remediation
all versions affected		See section Workarounds and Mitigations.
Control block CPX-CEC Codesys V2: Control block CPX-CEC Codesys V2 all versions affected	Festo:Ordercode:CPX-CEC, CPX-CEC-C1, CPX-CEC-M1	For CVE-2022-31806: Currently no fix is planned. For further mitigations see general recommendations. See section Workarounds and Mitigations.
Control block CPX-CEC Codesys V3: Control block CPX-CEC Codesys V3 all versions affected	Festo:Ordercode:CPX-CEC-C1-V3, CPX-CEC-S1-V3, CPX-CEC-M1-V3	For CVE-2022-22515: Currently no fix is planned. For further mitigations see general recommendations. See section Workarounds and Mitigations.
Control block CPX-CMXX: Control block CPX-CMXX all versions affected	Festo:Partnumber:555667, 555668 Festo:Ordercode:CPX-CMXX	For CVE-2022-31806: Currently no fix is planned. For further mitigations see general recommendations. See section Workarounds and Mitigations.
Controller CPX-E-CEC: Controller CPX-E-CEC all versions affected	Festo:Ordercode:CPX-E-CEC-C1, CPX-E-CEC-C1-PN, CPX-E-CEC-C1-EP, CPX-E-CEC-M1, CPX-E-CEC-M1-PN, CPX-E-CEC-M1-EP	For CVE-2022-22515: Currently no fix is planned. For further mitigations see general recommendations. See section Workarounds and Mitigations.
Compact Vision System SBO..-Q: Compact Vision System SBO..-Q all versions affected	Festo:Ordercode:SBO*-Q-*	For CVE-2022-31806: Currently no fix is planned. For further mitigations see general recommendations. See section Workarounds and Mitigations.
Controller FED-CEC: Controller FED-	Festo:Partnumber:559869 Festo:Ordercode:FED-CEC	For CVE-2022-31806: Currently no fix is planned. For further mitigations see general recommendations.

Affected Product and Versions	Product Details	Remediation
CEC all versions affected		See section Workarounds and Mitigations.

Workarounds and Mitigations

Festo has identified the following compensatory measures to reduce the risk:

- For CVE-2022-22515: Using the online user management prevents an attacker from downloading and execute malicious code, but also suppresses start, stop, debug, or other actions on a known working application that could potentially disrupt a machine or system.
- For CVE-2022-31806: Enable password protection at login in case no password is set at the controller.
  Please note that the password configuration file is not covered via default FFT backup & Restore mechanism, you must select the related file manually.

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-2022-22515
A remote, authenticated attacker could utilize the control program of the CODESYS Control runtime system to use the vulnerability in order to read and modify the configuration file(s) of the affected products.
Weakness: Exposure of Resource to Wrong Sphere (CWE-668)
Base Score: 8.1
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
CVE-2022-31806
In CODESYS V2 PLCWinNT and Runtime Toolkit 32 in versions prior to V2.4.7.57 password protection is not enabled by default and there is no information or prompt to enable password protection at login in case no password is set at the controller.
Weakness: Insecure Default Initialization of Resource (CWE-1188)
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

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

Further References

For further information also refer to:

- VDE-2022-037
- 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	November 29th, 2022	Initial version
1.0.1	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.