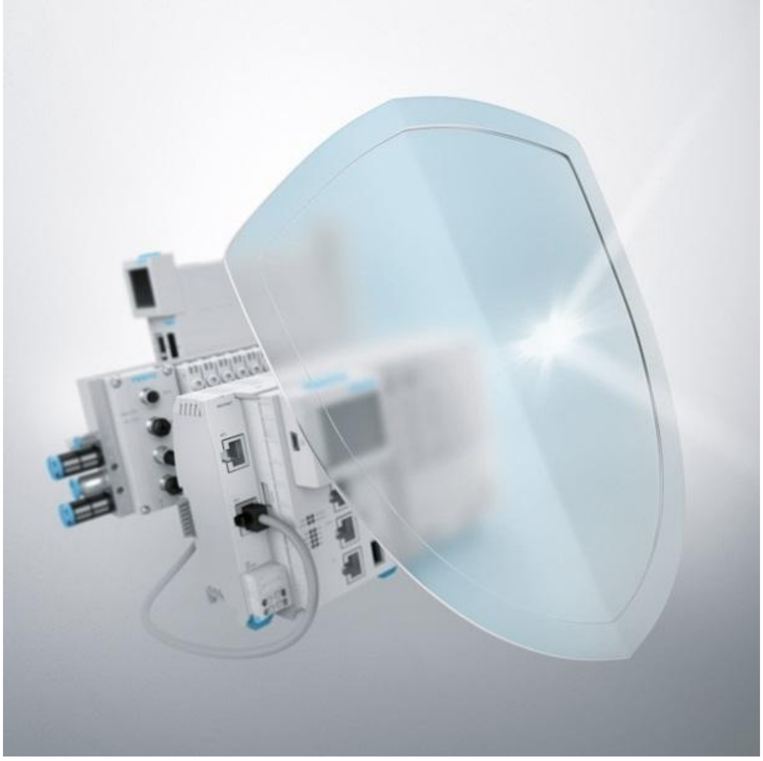
Several Codesys Vulnerabilities in Festo Products



fsa-202401

Date

January 30th, 2024

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

Several high severity vulnerabilities in CODESYS V3 affecting Festo products could lead to Remote Code Execution or Denial of Service.

Vulnerability Identifier

CVEs: CVE-2022-47378, CVE-2022-47379, CVE-2022-47380, CVE-2022-47381, CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47385, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390, CVE-2022-47391, CVE-2022-47392, CVE-2022-47393

Severity

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

Affected Vendors

FESTO

Affected Products and Remediations

Affected Product and Versions	Product Details	Remediation
CECC-X: CECC-X Gen 4: CECC-X Firmware <=4.0.18 affected	Festo:Partnumber:8124922, 8124923, 8124924 Festo:Ordercode:CECC-X-M1, CECC-X-M1-MV, CECC-X-M1-MV-S1	For all vulnerability identifiers: Update planned end of Q3 2024.
CECC-X: CECC-X Gen 3: CECC-X Firmware <=3.8.18 affected	Festo:Partnumber:4407603, 4407605, 4407606 Festo:Ordercode:CECC-X-M1, CECC-X-M1-MV, CECC-X-M1-MV-S1	For all vulnerability identifiers: No fix is planned. Please consider the general recommendations. See section Workarounds and Mitigations.

Affected Product and Versions	Product Details	Remediation
CPX-E-CEC: CPX-E-CEC >=8: CPX-E-CEC Firmware 3.2.10 affected	Festo:Partnumber:4252741, 4252742, 4252743, 4252744 Festo:Ordercode:CPX-E-CEC-C1-PN, CPX-E-CEC-C1-EP, CPX-E-CEC-M1-PN, CPX-E-CEC-M1-EP	For all vulnerability identifiers: Update planned end of Q3 2024.
CPX-E-CEC: CPX-E-CEC <8: CPX-E-CEC Firmware 2.2.14 affected	Festo:Partnumber:4252741, 4252742, 4252743, 4252744 Festo:Ordercode:CPX-E-CEC-C1-PN, CPX-E-CEC-C1-EP, CPX-E-CEC-M1-PN, CPX-E-CEC-M1-EP	For all vulnerability identifiers: Update planned end of Q3 2024.
CPX-E-CEC: CPX-E-CEC <=5: CPX-E-CEC Firmware <=10.1.4 affected	Festo:Partnumber:5226780, 5266781 Festo:Ordercode:CPX-E-CEC-C1, CPX-E-CEC-M1	For all vulnerability identifiers: Update planned end of Q3 2024.
CPX-CEC: CPX-CEC <=8: CPX-CEC Firmware <=4.0.4 affected	Festo:Partnumber:3473128, 3472765, 3472425 Festo:Ordercode:CPX-CEC-C1-V3, CPX-CEC-M1-V3, CPX-CEC-S1-V3	For all vulnerability identifiers: Update planned end of Q3 2024.
CECC-D: CECC-D <=7: CECC-D Firmware <=2.4.2 affected	Festo:Partnumber:574415, 8072995, 2463301 Festo:Ordercode:CECC-D, CECC-D-BA, CECC-D-CS	For all vulnerability identifiers: The product was discontinued in Aug 23. No fix is planned. Please consider the general recommendations. See section Workarounds and Mitigations.
CDPX-X: CDPX-X all versions: CDPX-X Firmware <=3.5.7.159 affected	Festo:Partnumber:574412, 574413, 574410, 574411, 8155216, 8155217, 8155218 Festo:Ordercode:CDPX-X-A-S-10, CDPX-X-A-W-13, CDPX-X-A-W-4, CDPX-X-A-W-7, CDPX-X-E1-W-7, CDPX-X-E1-W-10, CDPX-X-E1-W-15	For all vulnerability identifiers: Update planned end of Q3 2024.

Affected Product and Versions	Product Details	Remediation
CECC-LK: CECC-LK <=7: CECC-LK Firmware <=2.4.2 affected	Festo:Partnumber:574418 Festo:Ordercode:CECC-LK	For all vulnerability identifiers: The product was discontinued in Aug 23. No fix is planned. Please consider the general recommendations. See section Workarounds and Mitigations.
CECC-S: CECC-S <=7: CECC-S Firmware <=2.4.2 affected	Festo:Partnumber:574416 Festo:Ordercode:CECC-S	For all vulnerability identifiers: The product was discontinued in Aug 23. No fix is planned. Please consider the 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-2022-47378
After successful authentication, specific crafted communication requests with inconsistent content can cause the CmpFiletransfer component to read internally from an invalid address, potentially leading to a denial-of-service condition.
Weakness: Improper Validation of Consistency within Input (CWE-1288)
Base Score: 6.5
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CVE-2022-47379
After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to memory, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
Weakness: Out-of-bounds Write (CWE-787)

Base Score: 6.5
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CVE-2022-47380
After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
Weakness: Stack-based Buffer Overflow (CWE-121)
Base Score: 8.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-47381
After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
Weakness: Stack-based Buffer Overflow (CWE-121)
Base Score: 8.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-47382
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
Weakness: Stack-based Buffer Overflow (CWE-121)
Base Score: 8.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-47383
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
Weakness: Stack-based Buffer Overflow (CWE-121)
Base Score: 8.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-47384
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
Weakness: Stack-based Buffer Overflow (CWE-121)
Base Score: 8.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-47385
After successful authentication, specific crafted communication requests can cause the CmpAppForce component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
Weakness: Stack-based Buffer Overflow (CWE-121)

Base Score: 8.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-47386
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
Weakness: Stack-based Buffer Overflow (CWE-121)
Base Score: 8.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-47387
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
Weakness: Stack-based Buffer Overflow (CWE-121)
Base Score: 8.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-47388
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
Weakness: Stack-based Buffer Overflow (CWE-121)
Base Score: 8.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-47389
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
Weakness: Stack-based Buffer Overflow (CWE-121)
Base Score: 8.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-47390
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
Weakness: Stack-based Buffer Overflow (CWE-121)
Base Score: 8.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-47391
CODESYS products such as the CODESYS Control runtime systems contain communication servers for the
CODESYS protocol to enable communication with clients like the CODESYS Development System. Specific

crafted communication requests with inconsistent content can cause the CmpDevice component to read
internally from an invalid address, potentially leading to a denial-of-service condition.
Weakness: Improper Validation of Consistency within Input (CWE-1288)
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
CVE-2022-47392
After successful authentication, specific crafted communication requests with inconsistent content can cause the CmpApp/CmpAppBP/CmpAppForce components to read internally from an invalid address, potentially leading to a denial-of-service condition.
Weakness: Improper Validation of Consistency within Input (CWE-1288)
Base Score: 6.5
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CVE-2022-47393
After successful authentication, specific crafted communication requests can cause the CmpFiletransfer component to dereference addresses provided by the request for internal read access, which can lead to a denial-of-service situation.
Weakness: Untrusted Pointer Dereference (CWE-822)
Base Score: 6.5
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/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/)

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-2023-063
- CERT@VDE Security Advisories https://cert.vde.com/en/advisories/vendor/festo/
- Codesys Security Advisory 2023-02 https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17554&token=5444f53b4c90fe37043671a100dffa75305d1825&download=
- Codesys Security Advisory 2023-03 https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17555&token=212fc7e39bdd260cab6d6ca84333d42f50bcb3da&download=

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	January 30th, 2024	Initial version

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.