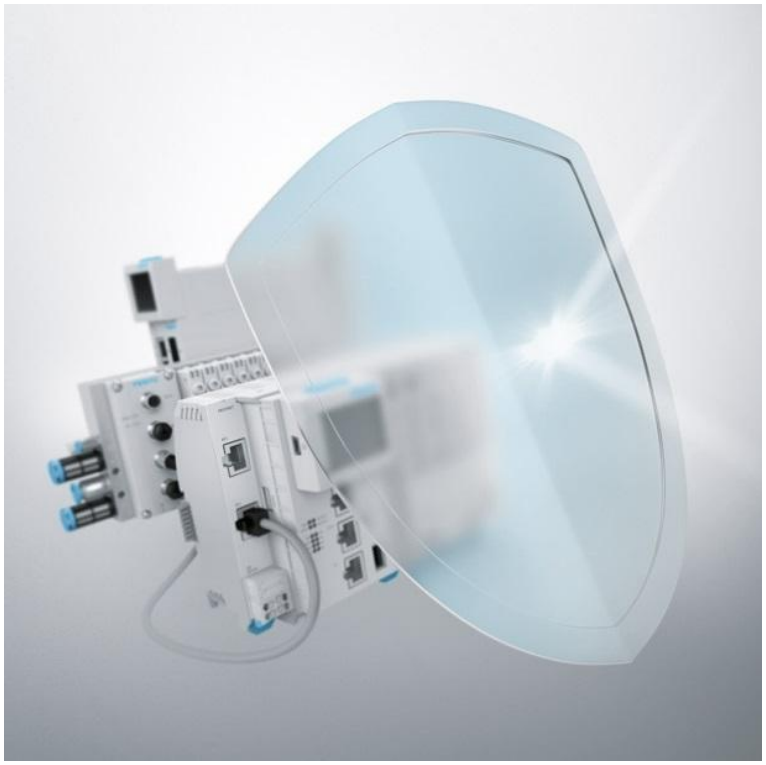
Festo Controller CECC-S,-LK,-D Family Firmware = 2.4.2.0 - Multiple Vulnerabilities in CODESYS V3 Runtime System



FSA-202203

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 Festo controller CECC product family is affected by multiple vulnerabilities in the CODESYS V3 runtime.

Vulnerability Identifier

CVEs: CVE-2019-5105, CVE-2019-9011, CVE-2019-9013, CVE-2020-10245, CVE-2020-12067, CVE-2020-12068, CVE-2020-12069, CVE-2020-15806, CVE-2021-29241, CVE-2021-29242, CVE-2021-33485, CVE-2021-36763, CVE-2021-36764, CVE-2022-22513, CVE-2022-22514, CVE-2022-22515, CVE-2022-22517, CVE-2022-22519

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-S: Firmware R07 (07.06.2021) = 2.4.2.0 affected	Festo:Partnumber:574416 Festo:Ordercode:CECC-S Modelnumber: CECC-S Rev4, CECC-S Rev5, CECC-S Rev6	For all vulnerability identifiers: No fix planned. This issue will be handled with next hardware generation release. See section Workarounds and Mitigations.
Controller CECC-LK: Firmware R07 (07.06.2021) = 2.4.2.0 affected	Festo:Partnumber:574418 Festo:Ordercode:CECC-LK Modelnumber: CECC-LK Rev4, CECC-LK Rev5, CECC-LK Rev6	For all vulnerability identifiers: No fix planned. This issue will be handled with next hardware generation release. See section Workarounds and Mitigations.

Affected Product and Versions	Product Details	Remediation
Controller CECC-D: Firmware R07 (07.06.2021) = 2.4.2.0 affected	Festo:Partnumber:574415 Festo:Ordercode:CECC-D Modelnumber: CECC-D Rev4, CECC-D Rev5, CECC-D Rev6	For all vulnerability identifiers: No fix planned. This issue will be handled with next hardware generation release. 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-2019-5105
An exploitable memory corruption vulnerability exists in the Name Service Client functionality of 3S-Smart Software Solutions CODESYS GatewayService. A specially crafted packet can cause a large memcpy, resulting in an access violation and termination of the process.
Weakness: Out-of-bounds Write (CWE-787)
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-2019-9011
This vulnerability enables valid user names to be identified.
Base Score: 5.3
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVE-2019-9013
An issue was discovered in 3S-Smart CODESYS V3 products. The application may utilize non-TLS based encryption, which results in user credentials being insufficiently protected during transport.
Weakness: Use of a Broken or Risky Cryptographic Algorithm (CWE-327)
Base Score: 8.8
Vector String: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2020-10245
CODESYS V3 web server before 3.5.15.40, as used in CODESYS Control runtime systems, has a buffer overflow.
Weakness: Out-of-bounds Write (CWE-787)
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-2020-12067
The user password can be changed without having to enter the original password.
Base Score: 7.5
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CVE-2020-12068
An issue was discovered in CODESYS Development System before 3.5.16.0. CODESYS WebVisu and CODESYS Remote TargetVisu are susceptible to privilege escalation.
Base Score: 6.5
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVE-2020-12069
In CODESYS V3 products in all versions prior V3.5.16.0 containing the CmpUserMgr, the CODESYS Control runtime system stores the online communication passwords using a weak hashing algorithm. This can be used by a local attacker with low privileges to gain full control of the device.
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-2020-15806
Specifically crafted requests sent to the CODESYS Control runtime system can allocate arbitrary amounts of memory, causing the system to run out of memory and possibly crash.
Weakness: Allocation of Resources Without Limits or Throttling (CWE-770)
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-2021-29241
CODESYS Gateway 3 before 3.5.16.70 has a NULL pointer dereference that may result in a denial of service (DoS).
Weakness: NULL Pointer Dereference (CWE-476)
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-2021-29242
CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages.
Weakness: Improper Input Validation (CWE-20)
Base Score: 7.3
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
CVE-2021-33485
CODESYS Control Runtime system before 3.5.17.10 has a Heap-based Buffer Overflow.
Weakness: Out-of-bounds Write (CWE-787)
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-2021-36763
In CODESYS V3 web server before 3.5.17.10, files or directories are accessible to External Parties.
Weakness: Files or Directories Accessible to External Parties (CWE-552)

Base Score: 7.5
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2021-36764
In CODESYS Gateway V3 before 3.5.17.10, there is a NULL Pointer Dereference. Crafted communication requests may cause a Null pointer dereference in the affected CODESYS products and may result in a denial-of-service condition.
Weakness: NULL Pointer Dereference (CWE-476)
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-2022-22513
The CODESYS protocol communication servers allow authenticated manipulated requests to dereference null pointers or provided untrusted pointers.
Weakness: NULL Pointer Dereference (CWE-476)
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-2022-22514
An authenticated, remote attacker can gain access to a dereferenced pointer contained in a request. The accesses can subsequently lead to local overwriting of memory in the CmpTraceMgr, whereby the attacker can neither gain the values read internally nor control the values to be written. If invalid memory is accessed, this results in a crash.
Weakness: Untrusted Pointer Dereference (CWE-822)
Base Score: 7.1
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H
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-2022-22517
An unauthenticated, remote attacker can disrupt existing communication channels between CODESYS products by guessing a valid channel ID and injecting packets. This results in the communication channel to be closed.
Weakness: Small Space of Random Values (CWE-334)
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-2022-22519
The CODESYS web server is used by the CODESYS WebVisu to display CODESYS visualization screens in a web browser. Specific crafted HTTP or HTTPS requests may cause an internal buffer over-read, which could crash the web server task of the CODESYS Control runtime system.
Weakness: Buffer Over-read (CWE-126)

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

Festo strongly recommends to minimize and protect network access to connected devices with state of the art techniques and processes.
Festo also highly recommends to apply available firmware updates containig security related changes as soon as possible.
For a secure operation follow the recommendations in the product manuals.

Until Festo provides a firmware-update with CODESYS runtime patching the vulnerabilities general recommendation is to:
1. Do not use the CODESYS Web server of the Web-visualization.
2. The access to a PLC with an active webserver should be restricted on network level to participants for whom it is strictly necessary. Also, the PLC should never be exposed to the internet. Assist IT staff to block access (from outside of company network or from outside of virtual network assigned to machines) to PLC through existing network equipment (routers, firewalls etc) by blocking specific ports and protocols (UDP, TCP).
3. PLC with WEB server active shall only include visualization screens in the application that are intended for being accessed by operators of the CODESYS WebVisu and the CODESYS Remote TargetVisu.
4. Activation of the CODESYS device user management and visualization user management if Web visualization is used.
- With the activation of the user management on the device any online service requires an appropriate authentication. It is highly recommended to setup at least one administrator user. Moreover, a set of users belonging to the appropriate groups allow maintaining leveled access rights.
- Use the protection of the user management in the CODESYS visualization not only for the navigation elements but also for all elements that should be restricted to certain operators only.

As part of a security strategy, Festo supports the CODESYS GmbH recommended 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

For more information and general recommendations for protecting machines and plants, see also the CODESYS Security Whitepaper: https://customers.codesys.com/fileadmin/data/customers/security/CODESYS-Security-Whitepaper.pdf

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-2022-027
- CERT@VDE Security Advisories https://cert.vde.com/de/advisories/vendor/festo/

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	July 18th, 2022	Initial version.
1.0.1	January 11th, 2024	Adjust link to VDE Advisory, TLP and update some CVE information, where CVSS was not known before.

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.