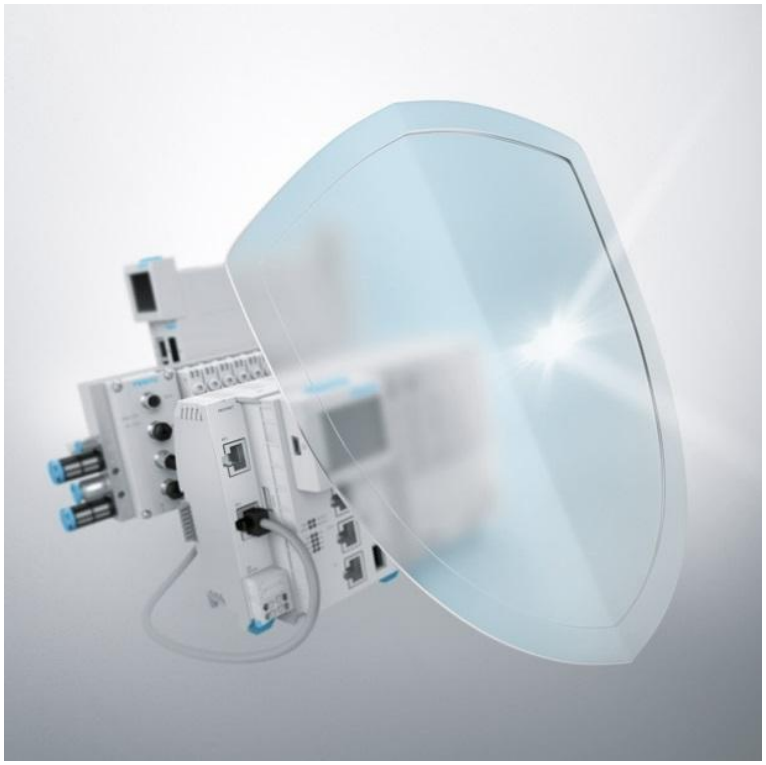
Festo Controller CECC-S,-LK,-D Family Firmware <= 2.3.8.1 - Multiple Vulnerabilities in CODESYS V3 Runtime System



FSA-202202

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

IDs: CODESYS Advisory 2017-01, CODESYS Advisory 2017-03, CODESYS Advisory 2017-06, CODESYS Advisory 2017-07, CODESYS Advisory 2017-09, CODESYS Advisory 2018-04, CODESYS Advisory 2018-05, CODESYS Advisory 2018-07, CODESYS Advisory 2018-11
CVEs: CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-5105, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9011, CVE-2019-9012, CVE-2019-9013, CVE-2019-13532, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2020-7052, 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

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

Affected Vendors

FESTO

Affected Products and Remediations

Affected Product and Versions	Product Details	Remediation
Controller CECC-S: Firmware R06 (11.10.2016) = 2.3.8.1 affected	Festo:Partnumber: 574416 Festo:Ordercode:CECC-S Modelnumber: CECC-S Rev4, CECC-S Rev5, CECC-S Rev6	For CODESYS Advisory 2017-01, CODESYS Advisory 2017-03, CODESYS Advisory 2017-06, CODESYS Advisory 2017-07, CODESYS Advisory 2017-09, CODESYS Advisory 2018-04, CODESYS Advisory 2018-05, CODESYS Advisory 2018-07, CODESYS Advisory 2018-11, CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9012, CVE-2019-13532, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2020-7052:

Affected Product and Versions	Product Details	Remediation
		Update to version 2.4.2.0 For 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: No fix planned. This issue will be handled with next hardware generation release. See section Workarounds and Mitigations.
Controller CECC-S: Firmware R05 (17.06.2016) = 2.3.8.0 affected	Festo:Partnumber: 574416 Festo:Ordercode:CECC-S Modelnumber: CECC-S Rev4, CECC-S Rev5, CECC-S Rev6	For CODESYS Advisory 2017-01, CODESYS Advisory 2017-03, CODESYS Advisory 2017-06, CODESYS Advisory 2017-07, CODESYS Advisory 2017-09, CODESYS Advisory 2018-04, CODESYS Advisory 2018-05, CODESYS Advisory 2018-07, CODESYS Advisory 2018-11, CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9012, CVE-2019-13532, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2020-7052: Update to version 2.4.2.0 For 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: No fix planned. This issue will be handled with next hardware generation release. See section Workarounds and Mitigations.
Controller CECC-LK: Firmware R06 (11.10.2016) =	Festo:Partnumber: 574418 Festo:Ordercode:CECC-LK Modelnumber: CECC-LK	For CODESYS Advisory 2017-01, CODESYS Advisory 2017-03, CODESYS Advisory 2017-06, CODESYS Advisory 2017-07, CODESYS Advisory 2017-09, CODESYS Advisory 2018-04, CODESYS Advisory

Affected Product and Versions	Product Details	Remediation
2.3.8.1 affected	Rev4, CECC-LK Rev5, CECC-LK Rev6	2018-05, CODESYS Advisory 2018-07, CODESYS Advisory 2018-11, CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9012, CVE-2019-13532, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2020-7052: Update to version 2.4.2.0 For 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: No fix planned. This issue will be handled with next hardware generation release. See section Workarounds and Mitigations.
Controller CECC-LK: Firmware R05 (17.06.2016) = 2.3.8.0 affected	Festo:Partnumber: 574418 Festo:Ordercode:CECC-LK Modelnumber: CECC-LK Rev4, CECC-LK Rev5, CECC-LK Rev6	For CODESYS Advisory 2017-01, CODESYS Advisory 2017-03, CODESYS Advisory 2017-06, CODESYS Advisory 2017-07, CODESYS Advisory 2017-09, CODESYS Advisory 2018-04, CODESYS Advisory 2018-05, CODESYS Advisory 2018-07, CODESYS Advisory 2018-11, CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9012, CVE-2019-13532, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2020-7052: Update to version 2.4.2.0 For 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: No fix planned. This issue will be handled with next

Affected Product and Versions	Product Details	Remediation
		hardware generation release. See section Workarounds and Mitigations.
Controller CECC-D: Firmware R06 (11.10.2016) = 2.3.8.1 affected	Festo:Partnumber: 574415 Festo:Ordercode:CECC-D Modelnumber: CECC-D Rev4, CECC-D Rev5, CECC-D Rev6	For CODESYS Advisory 2017-01, CODESYS Advisory 2017-03, CODESYS Advisory 2017-06, CODESYS Advisory 2017-07, CODESYS Advisory 2017-09, CODESYS Advisory 2018-04, CODESYS Advisory 2018-05, CODESYS Advisory 2018-07, CODESYS Advisory 2018-11, CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9012, CVE-2019-13532, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2020-7052: Update to version 2.4.2.0 For 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: No fix planned. This issue will be handled with next hardware generation release. See section Workarounds and Mitigations.
Controller CECC-D: Firmware R05 (17.06.2016) = 2.3.8.0 affected	Festo:Partnumber: 574415 Festo:Ordercode:CECC-D Modelnumber: CECC-D Rev4, CECC-D Rev5, CECC-D Rev6	For CODESYS Advisory 2017-01, CODESYS Advisory 2017-03, CODESYS Advisory 2017-06, CODESYS Advisory 2017-07, CODESYS Advisory 2017-09, CODESYS Advisory 2018-04, CODESYS Advisory 2018-05, CODESYS Advisory 2018-07, CODESYS Advisory 2018-11, CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9012, CVE-2019-13532, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2020-7052: Update to version 2.4.2.0

Affected Product and Versions	Product Details	Remediation
		For 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: 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

Only showing details of vulnerabilities with critical severity, please see in the list of Vulnerability Identifier for a complete list.

CODESYS Advisory 2018-04
The CODESYS runtime system allows to access files outside the restricted working directory of the controller by online services.
Base Score: 9.9
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
CVE-2018-10612
In 3S-Smart Software Solutions GmbH CODESYS Control V3 products prior to version 3.5.14.0, user access management and communication encryption is not enabled by default, which could allow an attacker access to the device and sensitive information, including user credentials.
Weakness: Missing Encryption of Sensitive Data (CWE-311)
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-2019-9010
The CODESYS Gateway does not correctly verify the ownership of a communication channel.
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-2019-13548
CODESYS V3 web server, all versions prior to 3.5.14.10, allows an attacker to send specially crafted http or https requests which could cause a stack overflow and create a denial-of-service condition or allow remote code execution.
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-2019-18858
CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.
Weakness: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (CWE-120)
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-2020-10245
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-2020-12069
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-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

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/
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-2022-022
- 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	July 15th, 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.