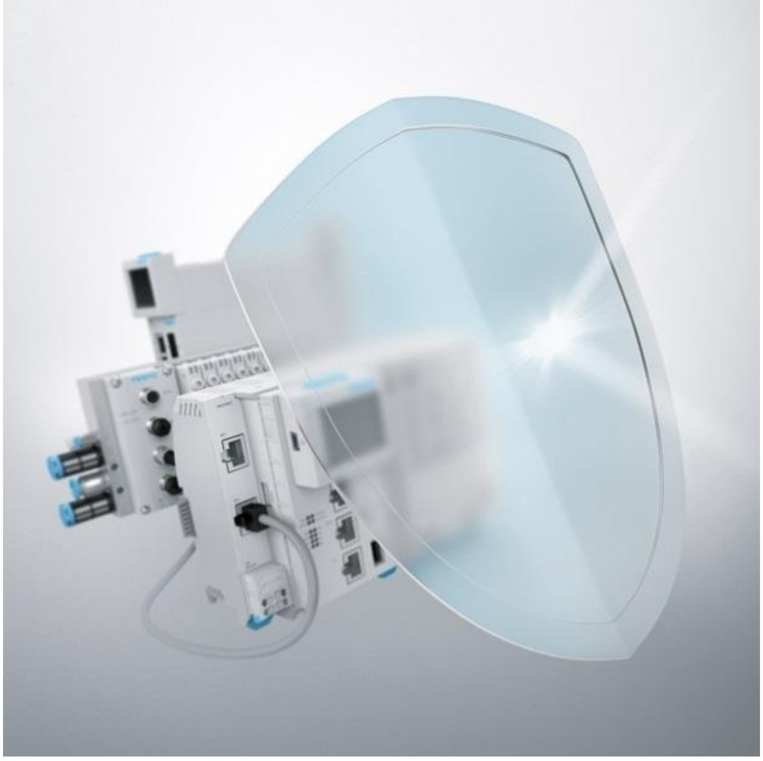
Several Codesys Gateway v2 vulnerabilities in Codesys provided by Festo



FSA-202406

Date
December 03rd, 2024

Creator
Festo SE & Co. KG

Version
2.0.0

Festo SE & Co. KG

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

Summary

An unauthenticated attacker would be able to send crafted requests to cause the CODESYS Gateway Server V2 to allocate excessive memory or consume all available TCP client connections. Besides, passwords are insufficiently checked during login.

All versions of the following CODESYS V2 product prior version V2.3.9.38 are affected:

- CODESYS Gateway Server

The identified vulnerabilities could lead to denial-of-service attacks, exhaustion of TCP connections, and unauthorized access to the system.

Vulnerability Identifier

CVEs: CVE-2022-31802, CVE-2022-31803, CVE-2022-31804

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
CODESYS provided by Festo: CODESYS provided by Festo all versions affected		For all CVEs: Enable password protection at login in case no password is set at the controller. Please note that the password configuration file is not covered by the default FFT backup and restore mechanism. You must select the related file manually.

Workarounds and Mitigations

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

- For CVE-2022-31802, CVE-2022-31803, CVE-2022-31804: Enable password protection at login in case no password is set at the controller. Please note that the password configuration file is not covered by the default FFT backup and 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-2022-31802
In CODESYS Gateway Server V2 for versions prior to V2.3.9.38 only a part of the the specified password is been compared to the real CODESYS Gateway password. An attacker may perform authentication by specifying a small password that matches the corresponding part of the longer real CODESYS Gateway password.
Weakness: Partial String Comparison (CWE-187)
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-2022-31803
In CODESYS Gateway Server V2 an insufficient check for the activity of TCP client connections allows an unauthenticated attacker to consume all available TCP connections and prevent legitimate users or clients from establishing a new connection to the CODESYS Gateway Server V2. Existing connections are not affected and therefore remain intact.
Weakness: Uncontrolled Resource Consumption (CWE-400)
Base Score: 5.3
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
CVE-2022-31804
The CODESYS Gateway Server V2 does not verifiy that the size of a request is within expected limits. An unauthenticated attacker may allocate an arbitrary amount of memory, which may lead to a crash of the Gateway due to an out-of-memory condition.
Weakness: Memory Allocation with Excessive Size Value (CWE-789)
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://certvde.com/)

Publisher Details

https://festo.com
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:

- CERT@VDE Security Advisories https://certvde.com/en/advisories/vendor/festo/
- FSA-202406: Several Codesys Gateway v2 vulnerabilities in Codesys provided by Festo - CSAF https://festo.csaf-tp.certvde.com/.well-known/csaf/white/2024/fsa-202406.json
- FSA-202406: Several Codesys Gateway v2 vulnerabilities in Codesys provided by Festo - HTML https://certvde.com/en/advisories/VDE-2024-059

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	December 03rd, 2024	Initial version
2.0.0	December 03rd, 2024	One reference has been corrected

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.