Advisory 2021-18

Security update for CODESYS Git

Published: 30 November 2021

Version: 1.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-18_GIT-529.docx

CONTENT

1 Affected Products

All versions of CODESYS Git prior V1.1.0.0 are affected by this vulnerability.

As CODESYS Git requires a CODESYS Development System version of V3.5.17.0 or newer, CODESYS Development Systems before V3.5.17.0 are not concerned at all.

2 Vulnerability overview

2.1 Type

CWE-295: Improper Certificate Validation [7]

2.2 Management Summary

CODESYS Git lacks server certificate validation using HTTPS protocol. Therefore, the server connection is vulnerable to a man-in-the-middle attack.

2.3 References

CVE: CVE-2021-34599 [6]

CODESYS JIRA: GIT-529

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.1 base score of 8.0 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Development System is an IEC 61131-3 programming tool for the industrial controller and automation technology sector. CODESYS Git seamlessly integrates the use of the distributed version control system Git™ into the CODESYS Development System.

Affected versions of CODESYS Git lack certificate validation in HTTPS handshakes. CODESYS Git does not implement certificate validation by default, so it does not verify that the server provides a valid and trusted HTTPS certificate. Since the certificate of the server to which the connection is made is not properly verified, the server connection is vulnerable to a man-in-the-middle attack.

3.2 Exploitability

This vulnerability could be exploited remotely.

3.3 Difficulty

An attacker with high skills would be able to exploit this vulnerability.

3.4 Existence of exploit

No known public exploits specifically target this vulnerability.

4 Available software updates

CODESYS GmbH has released CODESYS Git V1.1.0.0 to solve this vulnerability issue.

CODESYS Git V1.1.0.0 can be downloaded and installed directly with the CODESYS Installer. CODESYS Git requires a CODESYS Development System version of V3.5.17.0 or newer.

Alternatively, you can visit the CODESYS update area for more information on how to obtain the software update [3].

5 Mitigation

CODESYS GmbH recommends using the available software update to fix the vulnerability.

Currently, CODESYS GmbH has not identified any specific workarounds for this vulnerability, in case the software update is not applied.

As part of a security strategy, CODESYS GmbH 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
For more information and general recommendations for protecting machines and plants, see also the CODESYS Security Whitepaper [1].

6 Acknowledgments

CODESYS GmbH thanks those in the security community, who help us to improve our products and to protect customers and users through coordinated vulnerability disclosure.

This vulnerability was found internally by the CODESYS Security Team.

7 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact the CODESYS support team [5].

8 Disclaimer

CODESYS GmbH 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 on good faith by CODESYS GmbH. Insofar as permissible by law, however, none of this information shall establish any guarantee, commitment or liability on the part of CODESYS GmbH.

Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact sales@codesys.com.

Bibliography

[1] CODESYS GmbH: CODESYS Security Whitepaper
[2] CODESYS GmbH: Coordinated Disclosure Policy
[3] CODESYS GmbH update area: https://www.codesys.com/download
[4] CODESYS GmbH security information page: https://www.codesys.com/security
[5] CODESYS GmbH support contact site: https://www.codesys.com/support
[6] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[7] Common Weakness Enumeration (CWE): https://cwe.mitre.org
[8] CVSS Calculator: https://www.first.org/cvss/calculator/3.1
[9] ICS-CERT: https://ics-cert.us-cert.gov

The latest version of this document can be found here:

https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16959&token=3ce11e44a3277c4520d732ea2e630f2e06bd46ff&download=

Change History

Version	Description	Date
1.0	First version	30.11.2021