Advisory 2021-14

Security update for CODESYS EtherNetIP

Published: 22 July 2021

Version: 2.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-14_EIP-2.docx

CONTENT

1 Affected Products

All CODESYS EtherNetIP versions from V3.5.16.0 and before V4.1.0.0 inject this vulnerability into the generated code. This vulnerable protocol stack is downloaded to and executed by CODESYS Control runtime systems when they are configured as EtherNet/IP adapters.

CODESYS EtherNetIP versions prior to V3.5.17.0 were provided as integrated plugins of the CODESYS Development System. This means that all CODESYS Development System versions from V3.5.16.0 and before V3.5.17.0 generate vulnerable code for the EtherNet/IP adapter protocol stack.

As of CODESYS Development System V3.5.17.0, CODESYS EtherNetIP is provided as an optional AddOn and can be updated separately. CODESYS EtherNetIP V4.0.0.0 was the first version to be made available as an optional AddOn and delivered together with CODESYS Development System V3.5.17.0. Thus, the EtherNetIP AddOn versions from V4.0.0.0 and before V4.1.0.0 generate vulnerable code for the EtherNet/IP adapter protocol stack.

2 Vulnerability overview

2.1 Type

CWE-476: NULL Pointer Dereference [7]

2.2 Management Summary

Specific EtherNet/IP requests may cause a null pointer dereference in the downloaded vulnerable EtherNet/IP stack that is executed by the CODESYS Control runtime system.

2.3 References

CVE: CVE-2021-36765 [6]

CODESYS JIRA: EIP-2

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as medium.

The CVSS v3.0 base score of 5.8 has been assigned. The CVSS vector string is (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/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. It contains an integrated compiler for generating code for execution on the CODESYS Control runtime systems. CODESYS EtherNetIP is a fully integrated configurator, protocol stack & diagnostic tool for EtherNet/IP. A flaw within a CODESYS EtherNetIP adapter protocol stack library implies the vulnerability in the generated code. This vulnerable protocol stack is downloaded to and executed by CODESYS Control runtime systems when configured as

EtherNet/IP adapters.

Specific EtherNet/IP requests may cause a null pointer dereference in the downloaded vulnerable EtherNet/IP stack that is executed by the CODESYS Control runtime system, which in turn may cause a denial of service condition.

This issue only affects CODESYS projects that contain an EtherNet/IP adapter configuration.

3.2 Exploitability

This vulnerability could be exploited remotely.

3.3 Difficulty

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

3.4 Existence of exploit

No known public exploits specifically target this vulnerability. However, existing EtherNet/IP scanners may cause harm to the affected CODESYS products.

4 Available software updates

CODESYS GmbH has released version V4.1.0.0 of CODESYS EtherNetIP to solve the noted vulnerability issue. CODESYS EtherNetIP V4.1.0.0 can be downloaded and installed directly with the CODESYS Installer. This requires a CODESYS Development System version of V3.5.17.0 or newer. Older CODESYS Development System versions must be updated first.

To make the fix effective for existing CODESYS projects, you must additionally update the local EtherNet/IP adapter in the device tree to the latest version and perform a download of the CODESYS application to the PLC.

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

This issue was discovered by a CODESYS user.

CODESYS GmbH thanks for reporting following coordinated disclosure. This helps us to improve our products and to protect customers and users.

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

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/3.0
[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=16806&token=3b0c51de5a6e35bccbb413ddaaa56551ca5490f6&download=

Change History

Version	Description	Date
1.0	First version	15.07.2021
2.0	Software update available, CVE added	22.07.2021