Advisory 2022-01

Security update for CODESYS PROFINET

Published: 27 January 2022

Version: 1.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2022-01_PN-286.docx

CONTENT

1 Affected Products

CODESYS PROFINET V4.2.0.0 is affected by this vulnerability. Other versions are not affected.

Since CODESYS Development System V3.5.17.0, CODESYS PROFINET is delivered together with the CODESYS Development System, but can be updated separately like all optional AddOns. The vulnerable protocol stack is downloaded to and executed by the CODESYS Control runtime systems.

As CODESYS PROFINET V4.2.0.0 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-476: NULL Pointer Dereference [7]

2.2 Management Summary

Specific requests may cause a null pointer dereference in the vulnerable CODESYS PROFINET stack that is downloaded to and executed by the CODESYS Control runtime system.

2.3 References

CVE: CVE-2022-22510 [6]

CODESYS JIRA: PN-286, PN-301

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.1 base score of 7.5 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). [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 PROFINET is a fully integrated configurator, protocol stack & diagnostic tool for PROFINET. A flaw within the integrated SNMP server (UDP port 161) of the CODESYS PROFINET 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 PROFINET Controller or PROFINET Device.

Specific SNMP requests may cause a null pointer dereference in the vulnerable CODESYS PROFINET protocol stack, which in turn may cause a denial of service condition.

This issue only affects CODESYS projects that contain a PROFINET Controller or a PROFINET Device.

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 SNMP clients may cause harm to the affected CODESYS products by accidental access.

4 Available software updates

CODESYS GmbH has released CODESYS PROFINET V4.2.1.0 to solve this vulnerability issue.

This version can be downloaded and installed directly with the CODESYS Installer. A CODESYS Development System version of V3.5.17.0 or newer is required.

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

To make the fix effective for existing CODESYS projects, you must additionally update the local PROFINET Controller and/or PROFINET Device 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].

Template: templ_tecdoc_en_V3.0.docx

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.

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=17020&token=9acf91a2b5e1719ff71a019e86c3e8e411bfd252&download=

Change History

Version	Description	Date
1.0	First version	27.01.2022