Advisory 2016-03

CODESYS V3

Security update for several CODESYS products using pthreads DLL

Published: April 28, 2017

Version: 3.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2016-03_CDS-52287.docx

CONTENT

1 Affected Products

The following products running on Microsoft Windows desktop and server operating systems are affected by this issue:

- CODESYS Development System: All versions from V3.5 SP3 up to V3.5 SP10
- CODESYS OPC Server: All versions from V3.5 up to V3.5 SP10
- CODESYS Gateway V3: All versions from V3.5 up to V3.5 SP10
- CODESYS Control Win V3: All versions from V3.5 up to V3.5 SP10
- CODESYS HMI: All versions from V3.5 SP3 up to V3.5 SP10
- CODESYS VisuClient: All versions from V3.5 SP7 up to V3.5 SP10.
- CODESYS RTE (all 32 bit derivatives): All versions from V3.5 SP3 up to V3.5 SP10, if the CODESYS TargetVisu is used

2 Vulnerability overview

2.1 Type

DLL Hijacking, Privilege escalation

2.2 Management Summary

All the affected products install and or use the pthreads DLL. The untrusted search path vulnerability in Pthreads-win32 allows local users to gain privileges.

2.3 References

CVE-2010-5250 (for vulnerability in POSIX Threads for Win32)

CODESYS JIRA: CDS-52287

2.4 Severity Rating

3S-Smart Software Solutions GmbH has rated this vulnerability as high.

The CVSS v3 base score of 7.8 has been assigned. The CVSS vector string is (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

All the affected products install and or use the pthreads DLL. They are used for either develop software for or to communicate with CODESYS programmable logic controllers. Furthermore the various CODESYS Control runtime systems running on Microsoft Windows desktop and server operating systems are also affected. A user of these CODESYS products might be tricked into loading a DLL into the affected processes which could execute arbitrary code with the rights of that process.

3.2 Exploitability

This vulnerability could be exploited locally.

3.3 Difficulty

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

3.4 Existence of exploit

No known public exploits specifically target this vulnerability in CODESYS products. But we assume that existing exploits against pthreads may also cause harm to the affected CODESYS products.

4 Available software updates

3S-Smart Software Solutions GmbH has released version V3.5 SP10 Patch1 for all affected CODESYS products to solve this vulnerability issue.

5 Mitigation

3S-Smart Software Solutions GmbH has not identified any workarounds for this vulnerability.

But 3S-Smart Software Solutions GmbH recommends as part of the mitigation strategy the following defensive measures to reduce the risk of exploitation of this vulnerability:

- 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
- Protect both development and control system from unauthorized access e. g. by means of the operating system
- 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

3S-Smart Software Solutions GmbH thanks those in the security community, who help us to improve our products and to protect customers and users through coordinated vulnerability disclosure.

We thank Craig Markovic of Bedrock Automation Platforms for reporting this vulnerability in CODESYS products following coordinated disclosure.

7 Further Information

For additional information regarding the CODESYS products, especially the above mentioned versions, or about the described vulnerability please contact the 3S-Smart Software Solutions support team [5].

8 Disclaimer

3S-Smart Software Solutions 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 3S-Smart Software Solutions GmbH. Insofar as permissible by law, however, none of this information shall establish any guarantee, commitment or liability on the part of 3S-Smart Software Solutions GmbH.

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

Bibliography

[1] 3S-Smart Software Solutions GmbH: CODESYS Security Whitepaper
[2] 3S-Smart Software Solutions GmbH: Coordinated Disclosure Policy
[3] 3S-Smart Software Solutions GmbH download area: https://www.codesys.com/download
[4] 3S-Smart Software Solutions GmbH security information page: https://www.codesys.com/security
[5] 3S-Smart Software Solutions GmbH support contact site: https://www.codesys.com/support-training
[6] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[7] CVSS Calculator: https://www.first.org/cvss/calculator/3.0
[8] ICS-CERT: https://ics-cert.us-cert.gov

The latest version of this document can be found here:
https://customers.codesys.com/fileadmin/data/customers/security/2016/Advisory2016-03_CDS-52287.pdf

Change History

Version	Description	Date
1.0	First version	15.12.2016
2.0	Software update available	14.02.2017
3.0	Formal rework	28.04.2017