Advisory 2018-001: TwinCAT 2 and 3.1 Kernel Driver Privilege Escalation

Publication Date	03/13/2018
Last Update	04/06/2018
Current Version	1.1
Relevance	High
CVE	CVE-2018-7502

Summary

Several kernel drivers of TwinCAT 2 and 3.1 allow privilege escalation to SYSTEM level if an attacker is able to execute low-privileged code on the target computer.

An update for TwinCAT 2 and 3.1 is available.

Appearance

- TwinCAT 3.1 Build 4022 <= 4022.4
- TwinCAT 2.11 R3 <= 2259
- TwinCAT 3.1 C++ / Matlab (TC1210/TC1220/TC1300/TC1320)

Description

Several kernel drivers lack proper validation of user-supplied pointer values. An attacker who is able to execute code on the target can use this vulnerability to obtain SYSTEM privileges.

Solution

- Update TwinCAT 3.1 Build 4022 to version >= 4022.14
- Update TwinCAT 2.11 R3 to version >= 2300
- Recompile TwinCAT 3.1 C++/Matlab modules after update.

Acknowledgement

Beckhoff Automation thanks for his support and efforts:

- Steven Seeley of Source Incite for coordinated disclosure.

Reporting vulnerabilities

Beckhoff Automation welcomes responsibly coordinated reports of vulnerabilities and Beckhoff will collaborate with reporting parties to fix vulnerabilities or mitigate threats.

Additional Resources

[1] A general guideline for Beckhoff IPC Security:
http://download.beckhoff.com/download/Document/product-security/ipc_security_en.pdf

[2] National Institute of Standards and Technology. CVE-2018-7502 in National Vulnerability Database, 2018. https://nvd.nist.gov/vuln/detail/CVE-2018-7502

History

V 1.0	03/13/2018	Publication
V 1.1	04/06/2018	Added Reference to CVE

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20, 33415 Verl, Germany
Phone: +49 (0) 52 46/9 63 - 0
E-Mail: product-securityincident@beckhoff.com
www.beckhoff.com