Beckhoff Security Advisory 2020-002: EtherLeak in TwinCAT RT network driver

Publication Date	06/16/2020 (June 16th 2020)
Last Update	11/10/2020 (November 10th 2020)
Current Version	1.1
Relevance	Medium
CVE-ID	CVE-2020-12494
VDE-ID	VDE-2020-019
CVSS 3.1	5.3 Medium (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Summary

In case an network interface sends Ethernet frames with payloads smaller than the minimum frame length, memory content is disclosed within the padding.

Appearance

All installations of TwinCAT, which contain the real time (RT) Ethernet drivers

- “TwinCAT Driver for Intel 825**4**x” (Tcl825**4**x.sys) before or equal file version
    - 3.1.0.3603 for TwinCAT 3.1 4024
    - 3.1.0.3512 for TwinCAT 3.1 4022
    - 2.11.0.2120 for TwinCAT 2.11 2350
- “TwinCAT Driver for Intel 825**5**x” (Tcl825**5**x.sys) before or equal file version
    - 3.1.0.3600 for TwinCAT 3.1 4024
    - 3.1.0.3500 for TwinCAT 3.1 4024
    - 2.11.0.2117 for TwinCAT 2.11 2350

These are included within TwinCAT versions before or equal:

- TwinCAT 3.1 4024.10
- TwinCAT 3.1 4022.32
- TwinCAT 2.11 2305

In turn these versions are included in the following images:

- All Embedded PCs (CX) with Windows 7 / 10 / CE
- All Industrial PCs with Windows 7 / 10 / CE, in case TwinCAT RT driver was enabled

Description

Beckhoff’s TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device.

Mitigation

If no real-time communication from TwinCAT is required on the Ethernet interface, then users can alternatively re-configure them to use the Intel ® driver, which is shipped with Beckhoff images.

Customers should configure a perimeter firewall to block traffic from untrusted networks to the device, especially regarding ICMP and other small ethernet frames.

Beckhoff offers software patches for TwinCAT 3.1 and TwinCAT 2.11 on request. These patches will be included in the the next regular releases to the affected software versions. The advisory will be updated upon availability.

Solution

Please update TwinCAT

- TwinCAT 2.11 to build 2306 or newer
- TwinCAT 3.1 to build 4024.11 or newer

Reporting vulnerabilities

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

Disclaimer

Beckhoff is not responsible for any side effects negatively affecting the real-time capabilities of your TwinCAT control application possibly caused by updates. Beckhoff offers updated images with qualified performance for Beckhoff hardware from time to time. TwinCAT System Manager offers tools which can be of assistance to verify real-time performance after update. A backup should be created every time before installing an update. Only administrators or IT experts should perform the backup and update procedure.

References

[1] Additional information about the latest IPC security advisories are provided here: www.beckhoff.com/secinfo

History

V 1.0	06/16/2020	Publication
V 1.1	11/10/2020	Added Solution