Beckhoff Security Advisory 2019-007:
Denial-of-Service on TwinCAT using Profinet protocol

Publication Date	10/07/2019
Last Update	08/04/2020
Current Version	1.1
Relevance	High
CVE-ID	CVE-2019-5637
VDE-ID	VDE-2019-019

Summary

In case TwinCAT is configured to use the Profinet driver, a denial of service of the controller could be reached by sending special packets to the device.

Appearance

All TwinCAT versions equal or below

- TwinCAT 2 Build 2304
- TwinCAT 3.1 Build 4024.0

Description

TwinCAT includes a Profinet driver, which could be configured in the engineering environment to use Profinet connections to the controller.

In case this is configured and the controller is started, a specially crafted Profinet DCP packet could be sent to the TwinCAT device, which will lead to a denial of service of the device.

Operation can be resumed by restarting the device.

Solution

Please update TwinCAT

- TwinCAT 2 to 2305 or newer
- TwinCAT 3.1 to 4024.4 or newer

Mitigation

If the solution is not applicable, Profinet could be configured in perimeter firewall to block PROFINET DCP packets from untrusted networks to the device.

Acknowledgement

Beckhoff Automation thanks Andreas Galauner from Rapid7 for support and efforts within coordinated disclousure.

Reporting vulnerabilities

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

History

V 1.0	10/07/2019	Publication
V 1.1	08/04/2020	Added Solution; Added VDE-ID