BECKHOFF New Automation Technology

Beckhoff Security Advisory 2019-07:
Denial-of-Service on TwinCAT using Profinet protocol

Publication Date	7/10/2019
Last Update	7/10/2019
Current Version	1.0
Relevance	High
Related CVE	CVE-2019-5637

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.

Mitigation

Profinet could be blocked in perimeter firewall to block PROFINET DCP packets from untrusted networks to the device.

Beckhoff will provide updates for the mentioned TwinCAT Versions.

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	07/10/2019	Publication