Beckhoff Security Advisory 2022-001:
Null Pointer Dereference vulnerability in products with OPC UA technology

Publication Date	01/03/2022 (Mar 1st 2022)
This Update	01/03/2022 (Mar 1st 2022)
This Version	1.1
Latest Version	https://download.beckhoff.com/ [...] /advisory-2022-001.pdf
VDE-ID	VDE-2022-003
CVE-ID	CVE-2021-45117
CVSS 3.1	6.5 Medium (AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)
Weakness Enumerator	CWE-476 NULL Pointer Dereference

Summary

By tricking clients of the mentioned products into contacting malicious OPC UA servers and thereby acting as OPC UA clients, a crash of the component can be provoked.

Appearance

Component	Included in product	Affected product version (BEFORE and NOT INCLUDING the named version)
TwinCAT OPC UA Server	TF6100-OPC-UA-Server	Setup version < 4.4.44 containing TcOpcUaServer version < 3.2.0.240
	TS6100-OPC-UA	Setup version < 4.4.0 containing TcOpcUaServer version < 3.2.0.240
	TS6100-0030-OPC-UA	Setup version < 4.4.0 containing TcOpcUaServer version < 3.2.0.240
TwinCAT OPC UA Client	TF6100-OPC-UA-Client	Setup version < 4.4.16 containing TcOpcUaClient version < 2.2.9.1
	TS6100-OPC-UA	Setup version < 4.4.0 containing TcOpcUaClient version < 2.2.9.1
	TS6100-0030-OPC-UA	Setup version < 4.4.0 containing TcOpcUaClient version < 2.2.9.1
TwinCAT OPC UA Gateway	TF6100-OPC-UA-Gateway	Setup version < 4.4.2 containing TcOpcUaGateway version < 1.5.8.454
	TS6100-OPC-UA	Setup version < 4.4.0 containing TcOpcUaGateway version < 1.5.8.454
	TS6100-0030-OPC-UA	Setup version < 4.4.0 containing TcOpcUaGateway version < 1.5.8.454
TwinCAT HMI OPC UA	TF2110	Setup version < 1.12.754.0
IPC Diagnostic UA Server	Contained in Beckhoff's Windows images	IPC Device Manager Setup version < 2.3.3.0 containing MDP UA Server < 3.1.0.8
TwinCAT OPC UA Server	EK9160	Firmware version < 3.00 containing TcOpcUaServer version < 3.2.0.239

Description

The above products can be used as clients which contact an OPC UA server. If such connection is made with SecurityMode=None for the connection then the client can receive a malformed message during the conversation which provokes a null pointer dereference within the OPC UA stack of the product. The product crashes then by memory access violation. Though this is uncommon and not recommended, such connections with SecurityMode=None may even be used by OPC UA Servers, for example if they act as client to register at a Discovery Server.

Mitigation

Have your applications configured to use other than SecurityMode=None for all OPC UA connections. Avoid that these connect to an unknown OPC UA server with SecurityMode=None. In particular, avoid that your applications connect to servers which they discover via mDNS, a Local Discovery Server (LDS), an untrusted Global Discovery Server (GDS) or even trusted GDS using SecurityMode=none. Especially in the latter case an adversary might be able to apply the “man in the middle” pattern to attack the connection and inject a bad message which triggers the vulnerability.

Solution

Please update to a recent version of the affected product.

Acknowledgement

Beckhoff Automation thanks the OPC Foundation and Unified Automation for reporting the issue and for support and efforts with the coordinated disclosure. Also Beckhoff Automation thanks CERT@VDE for coordination.

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 is provided here:
www.beckhoff.com/secinfo

History

V 1.0	01/03/2022	Publication
V 1.1	01/03/2022	Correction of product name “TS6100-OPC-UA”