BECKHOFF New Automation Technology

Beckhoff Security Advisory 2021-003:
Relative path traversal vulnerability through TwinCAT OPC UA Server

Publication Date	11/03/2021 (Nov 3rd 2021)
Last Update	11/03/2021 (Nov 3rd 2021)
Current Version	1.0
VDE-ID	VDE-2021-051
CVE-ID	CVE-2021-34594
CVSS 3.1	6.5 Medium (AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H)
Weakness Enumerator	CWE-23: Relative Path Traversal

Summary

Through specific nodes of the server configuration interface of the TwinCAT OPC UA Server administrators are able to remotely create and delete any files on the system which the server is running on, though this access should have been restricted to specific directories. In case that configuration interface is combined with not recommended settings to allow anonymous access via the TwinCAT OPC UA Server then this kind of file access is even possible for any unauthenticated user from remote.

Appearance

Component	Included in product	Affected product version (BEFORE and NOT INCLUDING the named version)
TwinCAT OPC UA Server	TF6100	TF6100 version < 4.3.48.0 containing TcOpcUaServer version < 3.2.0.194
TwinCAT OPC UA Server	TS6100	TS6100 version < 4.3.48.0 containing TcOpcUaServer version < 3.2.0.194

Description

The OPC UA server called “TcOpcUaServer” provides specific nodes within a specifc namespace which allow to configure features of that OPC UA server. By accessing some of these nodes an OPC UA client can create and delete configuration files for these features on behalf of the administrator of the “TcOpcUaServer”. For these files dedicated directories are used on the file system of the computer where the “TcOpcUaServer” is running. Affected versions were missing specific sanity checks for the file names used and an attacker could add relative paths to the file names to create and delete files outside of the dedicated directories.

The specific nodes reside within the OPC UA namespace which is identified by the following namespace URI:

http://beckhoff.com/TwinCAT/TF6100/Server/Configuration

With the default configuration the dedicated directories are the following on the system partition of the system where “TcOpcUAServer” is running:

TwinCAT\Functions\TF6100-OPC-UA\Server\res
TwinCAT\Functions\TF6100-OPC-UA\Server\xmlnodesets
TwinCAT\Functions\TF6100-OPC-UA\Server\symbolfiles

Please note that the default installation of the “TcOpcUAServer” does allow anonymous access even to the administrative nodes within the namespace described above. However, Beckhoff recommends to restrict access with the help of the various security features of the “TcOpcUaServer” as described with [2]. This is why operating the “TcOpcUAServer” with allowing anonymous access to the administrative nodes is not considered the intended use here.

Mitigation

Consider restricting access to the nodes of the “TcOpcUAServer” with the methods described by [2] such that the administrative interface can only be accessed by administrative users of well known OPC UA clients.

Solution

Please update to a recent version of the affected product.

Acknowledgement

Beckhoff Automation thanks Johannes Olegård, Emre Süren, and Robert Lagerström 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
[2] “Configuring security settings - Beckhoff Information System”
https://infosys.beckhoff.com › content › tcopcuaserver

History

V 1.0	11/03/2021	Publication