Beckhoff Security Advisory 2021-002:
Stack Overflow and XXE vulnerability in various OPC UA products

Publication Date	05/14/2021 (May 14th 2021)
Last Update	05/14/2021 (May 14th 2021)
Current Version	1.0
VDE-ID	VDE-2021-008
US ICS-ID	VU-131108
1st CVE-ID	CVE-2021-27432
1st CVSS 3.1	7.5 High (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
1st Weakness Enumerator	CWE-674: Uncontrolled Recursion
2nd CVE-ID	CVE-2021-27434
2nd CVSS 3.1	7.2 Medium (AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:L)
2nd Weakness Enumerator	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Summary

The affected products can act as OPC UA client or server and are vulnerable to two different kind of attacks via the OPC UA protocol. For both cases the attacker can send packets via the OPC UA protocol without the need to authenticate and

1. provoke a stack overflow resulting in denial of service of the product or
2. make the product disclose information to the attacker without authorization.

Appearance

Component	Included in product	Affected product version (BEFORE and NOT INCLUDING the named version)
TwinCAT Scope Server	TF3300	< TF3300 3.4.3144.11
TwinCAT OPC UA Configurator (Standalone)	TS6100 TF6100	< TS6100 4.3.46.0 < TF6100 4.3.46.0
TwinCAT OPC UA Configurator (Visual Studio)	TF6100	< TF6100 4.3.46.0
TwinCAT Target Browser OPC UA Extension	TF6100 TF6720 TF3300	< TF6100 4.3.46.0 < TF6720 1.1.68.0 < TF3300 3.4.3144.11
TwinCAT OPC UA Client System Manager Extension	TF6100	< TF6100 4.3.46.0
TwinCAT OPC UA Sample Client	TS6100 TF6100	< TS6100 4.3.46.0 < TF6100 4.3.46.0

Description

For both kinds of attacks the attacker needs to use a specifically crafted OPC UA client when attacking an OPC UA server respectively needs to use a specifically crafted OPC UA server when attacking an OPC UA client. For attacking a server the attacker needs to be able to establish a TCP connection to that server. For attacking a client the attacker needs to be able to make the client connect to the attacker's server. For all cases it is sufficient if after the establishment of the TCP connection the attacker lets the specifically crafted application (client or server) respond with a sequence of specifically crafted network packets. No authentication is required by the attacker.

For the first kind of attack the specifically crafted network packets cause a stack overflow as consequence of an uncontrolled recursion when the attacked application (client or server) processes them. With the components of the product described above, this attack results in a denial of service because the components become unavailable and need to be restarted manually after the attack.

For the second kind of attack the specifically crafted network packets cause the attacked application to resolve XML entities which allows the inclusion of contents from files on disk as far as they are accessible to the attacked application. Further processing of XML entities allow the resulting XML content to be posted to an HTTP server of the attackers choice. This allows the disclosure of file content from the computer the attacked application is running on even though the attacker is not required to authenticate nor to have access to these files.

The second attack is possible only if an outdated version of a .NET Framework from Microsoft is used. For more information like vulnerable and fixed versions of the .NET Framework, please see [2].

Since TCP connections are routable the attacker may perform all these kinds of exploits from remote if there is no firewall set up which limits the access for example to the TCP ports which the OPC UA application is using. The attacker does not need to have a local account at the device or OPC UA server nor is any authentication required for the attack.

Mitigation

Consider limiting access to the network communication ports of affected server products. Also consider limiting where the affected client products are allowed to connect to. For example, this can be achived with Windows' built-in firewall by incoming rules for servers and outgoing rules for clients.

Consider to minimize the ability of an attacker to hijack communication establishment from a client to a server. For example this can be achieved with the help of zones and conduits: Try to keep servers and clients within the same network zone and prevent intrusion into that zone. Try to enclose communication establishment within conduits like VPN channels (where one conduit can serve for many OPC UA connections) and prevent attackers from intruding into such channels.

Consider updating the .NET Framework.

Solution

Update to a recent version of the affected product and update the .NET Framework.

Acknowledgement

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] CVE-2015-6096 available at https://nvd.nist.gov/vuln/detail/CVE-2015-6096

History

V 1.0	05/14/2021	Publication