Beckhoff Security Advisory 2021-001:
DoS-Vulnerability for TwinCAT OPC UA Server and IPC Diagnostics UA Server

Publication Date	04/26/2021 (April 26th 2021)
Last Update	05/10/2021 (May 10th 2021)
Current Version	1.2
CVE-ID	CVE-2020-12526
VDE-ID	VDE-2020-051
CVSS 3.1	5.3 Medium (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
Weakness Enumeration	CWE-20: Improper Input Validation

Summary

Some TwinCAT OPC UA Server and IPC Diagnostics UA Server versions from Beckhoff Automation GmbH & Co. KG are vulnerable to denial of service attacks. The attacker needs to send several specifically crafted requests to the running OPC UA server. After some of these requests the OPC UA server is no longer responsive to any client. This is without effect to the real-time functionality of IPCs.

Appearance

- TwinCAT OPC UA Server (contained within TF6100 OPC UA)
  - server versions up to and including 2.3.0.12 are affected
    - these are included within TF6100 versions up to and including 3.3.18
  - Please note that some hardware products from Beckhoff are shipped with a TwinCAT OPC UA Server pre-installed. In some cases the server is enabled by default.
- IPC Diagnostics UA Server (contained in Beckhoff's Windows images)
  - server versions up to and including 3.1.0.1 are affected
  - Please note that IPC products from Beckhoff are shipped with an IPC Diagnostics UA Server pre-installed. While on Windows CE it is disabled by default all other Windows images have it enabled by default.

The version numbers named above always refer to the version number which is accessible via OPC UA at the server via the standard OPC UA node /Objects/Server/ServerStatus/BuildInfo/SoftwareVersion and on Windows also as the file property "File version" of the file TcOpcUaServer.exe for TwinCAT OPC UA Server respectively the file DevMgrSvr-UA.exe for IPC Diagnostics UA Server.

Description

An attacker who can establish a TCP connection to one of the affected OPC UA servers can send a series of specifically crafted data packets to it. By repeating this several times this will provoke a stack overflow at the OPC UA server which then stops and does not recover until restarted by an administrator.

Since TCP connections are routable there attacker may perform the exploit from remote if there is no firewall set up which limits the access to the TCP which the OPC UA server is listening on. The attacker does not need to have a local account at the device or OPC UA server nor it any authentication required for the attack.

Please note: The availability impact within the CVSS vector has been rated low because the TwinCAT OPC UA Server and IPC Diagnostics UA Server are seen as less-essential functional parts of an Industrial PC (IPC) image, not as its core functionality. The critical functionality of the IPC is its real-time runtime. The TwinCAT OPC UA Server is a communication interface. The IPC Diagnostics UA Server is for the hardware diagnostics functionality of the IPC. The main function of the IPC remains unaffected during the attack.

Mitigation

Consider disabling the IPC Diagnostics Server by stopping and disabling the corresponding Windows service or service. For example this can be achieved with the following PowerShell commands:

```
Stop-Service -Force -Name DevMgrSvr-UA
Set-Service -Name DevMgrSvr-UA -StartupType Disabled
```

Alternatively consider limiting access to the TCP port the OPC UA server is listening on. This can happen with a dedicated firewall appliance which sits in front of an affected device. Alternatively at the device the Windows firewall can be configured to limit access to the TCP port. Further guidance is provided within the “Security Guide IPC” from Beckhoff which is accessible at https://www.beckhoff.com/secguide .

Solution

For devices running Windows but not Windows CE or TwinCAT/BSD please get a recent version of the OPC UA servers through the conventional ways and update your system.

For devices running Windows CE please request a recent image via Beckhoff’s support and apply it to your device. For the product CX8091 please use firmware version “`CX8091_CE600_LF_v356f_TC211R3_B2306_v2`” or later which can be downloaded at

```
https://download.beckhoff.com/download/software/embPC-Control/CX80x0/CX8091/OPC-update
```

Please note that the updated OPC UA server leaves less RAM available to your application on the CX8091.

Acknowledgement

Beckhoff Automation thanks Industrial Control Security Laboratory of QI-ANXIN Technology Group Inc. from China 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	04/26/2021	Publication
V 1.1	04/26/2021	Added explanation for CVSS and acknowledgement for CERT@VDE
V 1.2	05/10/2021	Corrected explanation of default settings for Windows images