Beckhoff Security Advisory 2020-003:
Privilege Escalation through TwinCAT System Tray (TcSysUI.exe)

Publication Date	11/19/2020 (November 19th 2020)
Last Update	11/24/2020
Current Version	1.1
CVE-ID	CVE-2020-12510
VDE-ID	VDE-2020-037
CVSS 3.1	7.3 High (AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H)
Weakness Enumeration	CWE-276: Incorrect Default Permissions

Summary

The default installation path and its permissions for the TwinCAT runtime allow a local user to replace or modify executables other users of the same system might execute. The issue does not apply for installations underneath C:\Program Files.

Appearance

All installations of TwinCAT XAR 3.1 with default installation path.

Description

The default installation path of the TwinCAT software is underneath C:\TwinCAT. If the directory does not exist it and further subdirectories are created with permissions which allow every local user to modify the content. The default installation registers TcSysUI.exe for automatic execution upon log in of a user. If a less privileged user has a local account he or she can replace TcSysUI.exe. It will be executed automatically by another user during login. This is also true for users with administrative access. Consequently, a less privileged user can trick a higher privileged user into executing code he or she modified this way. By default Beckhoff's IPCs are shipped with TwinCAT software installed this way and with just a single local user configured. Thus the vulnerability exists if further less privileged users have been added.

Mitigation

Please consider the solution described with the next section (title "Solution") for new installations only and installations for which it is acceptable to reinstall TwinCAT.

For existing installations a script is provided for download at the following link:
https://download.beckhoff.com/download/Document/product-security/Advisories/advisory-2020-003/cve-2020-12510.zip

It changes the permissions of a directory of an already installed TwinCAT 3.1 installation. More precisely, it reads the current permissions of "C:\Program Files" and copies them to the directory "3.1\System" underneath the installation path of TwinCAT (default "C:\TwinCAT\3.1\System").

The procedure to use that script is as follows:

1) Download the script, unzip it, and copy it to the IPC.
2) On the IPC log in as administrator and open a PowerShell (Windows-Key + R + "PowerShell").
3) At the PowerShell enter the following command to temporarily allow the execution of scripts:
   ```
   set-executionpolicy -ExecutionPolicy Unrestricted -Scope Process
   ```
   (The effect of this is limited to the life-time of the current shell window because of "-Scope Process".)
4) Then change to the path to where you downloaded the script and execute it:
   ```
   .\cve-2020-12510.ps1
   ```
   The expected output is "`Copied the permissions from C:\Program Files to` <installPath>\3.1\System".
5) Close the PowerShell and log out from the IPC as needed.

It is safe to apply the script several times. It is safe to run it during full operation of TwinCAT XAR 3.1. There is no need to reboot the IPC afterwards.

There is no need to periodically run the script. Future updates of TwinCAT 3.1 will either not touch the permissions which are set by the script or apply more appropriate ones.

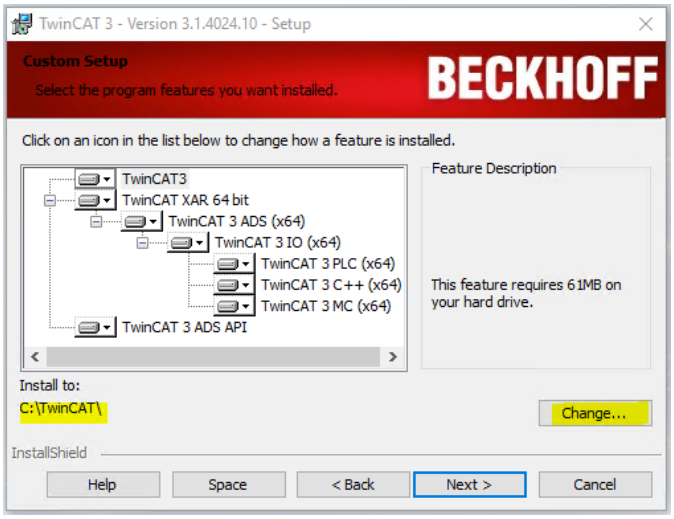
To apply the procedure to a set of IPCs you can prepare a USB stick with the content of the ZIP file “cve-2020-12510.zip” (see download URL above). Then the procedure for each IPC is:

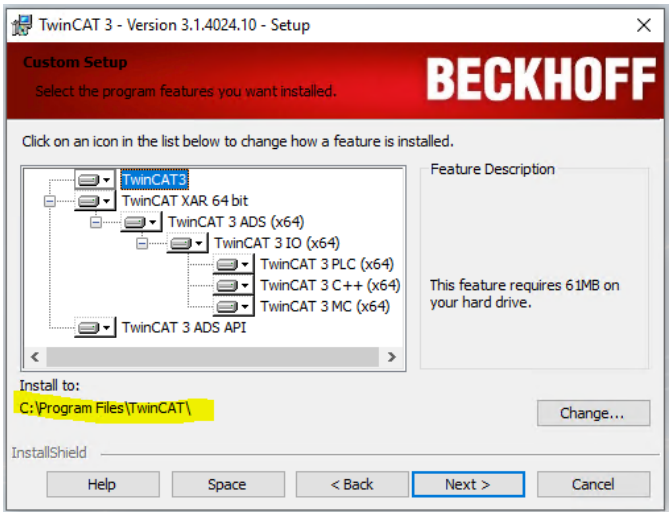
1) Log in as administrator on the IPC.
2) Open the USB stick with the File Explorer (formerly known as Windows Explorer).
3) Double click on the file “run-cve-2020-12510.bat”.
   (This simply invokes the PowerShell to execute the script already described above.)

Solution

Please consider the mitigation described with the section above for existing installations for operation.

Please consider to choose “C:\Program Files\TwinCAT” during installation of TwinCAT 3.1. If you have installed it already then please uninstall and re-install it with the changed path. Please use the custom installation for this. That will automatically protect the binaries such that they can only be modified by an administrator.





Please mind that already installed projects underneath C:\TwinCAT need to be moved. It is recommended to perform a backup of the complete device before such action. For security reasons, please remove the former content of C:\TwinCAT at the end of this sequence. This will also prevent confusion.

Acknowledgement

Beckhoff Automation thanks Ayushman Dutta for reporting the issue and for support and efforts with the coordinated disclosure.

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 are provided here:
www.beckhoff.com/secinfo

History

V 1.0	11/19/2020	Publication
V 1.1	11/24/2020	Added a mitigation