BECKHOFF New Automation Technology

Beckhoff Security Advisory 2025-001: Deserialization of untrusted data by TwinCAT 3 Engineering

Publication Date	09/09/2025 (Sept. 9th 2025)
This Update	09/09/2025 (Sept. 9th 2025)
This Version	1.0
Latest Version	PDF
VDE-ID	VDE-2025-075
CVE-ID	CVE-2025-41701
CVSS 3.1	7.8 High (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
Weakness Enumerator	CWE-502 Deserialization of Untrusted Data

Summary

An unauthenticated attacker can trick a local user into executing arbitrary commands by opening a deliberately manipulated project file with an affected engineering tool. These arbitrary commands are executed in the user context. When older affected versions of the engineering tool are installed then the deliberate manipulation of the project file can cause that these are used to open it.

Appearance

Component	Affected component version	Included in product	Affected product version
n/a – The issue does not reside in a component but the product itself.		TE1000 | TwinCAT 3 Engineering	< TwinCAT 3.1 Build 4024.67

Description

Beckhoff's TwinCAT 3 Engineering software is intented to craft automation projects consisting of a set of files which are stored locally as files underneath an individual folder or in a packed file. TwinCAT 3 Engineering stores such settings in files which are called “Solution User Options (.suo) File”. When such settings are manipulated or crafted by an adversary in a specific way then TwinCAT 3 Engineering executes arbitrary commands as determined by these settings when the user uses TwinCAT 3 Engineering to open the project. These arbitrary commands are executed in the user context.

Please note that solution user option files should not be checked in to source code control. This is also best practice when working with source code projects and solutions. For example, see [2] and [5].

Please note that TwinCAT 3 Engineering offers the “Remote Manager” feature (see [3]) which means that older versions of TwinCAT 3 Engineering can stay installed in parallel to more recent versions. Each older version is automatically available from the most recent version then as so called “Remote Manager”. TwinCAT projects can be “pinned” to be edited with a fixed version, see [4]. If such a pinned project is opened while a more recent version of TwinCAT 3 Engineering is installed and at the same time the matching older version of TwinCAT 3 Engineering is still installed then the project is automatically passed from the more recent version to the matching older version and edited with that older version where that older version is vulnerable.

The vulnerability is similar to older vulnerabilities that were addressed in the CODESYS Development System V3 product from CODESYS GmbH with CVE-2021-21864, CVE-2021-21865, CVE-2021-21866, CVE-2021-21867, CVE-2021-21868, CVE-2021-21869, and the associated Advisory 2021-13 from CODESYS GmbH.

Mitigation

Developers shall care for opening projects from trusted sources only. This is best practice when working with source code and the main content of a project which is crafted with TwinCAT 3 Engineering is source code which is to be compiled to activate it on a target.

Solution user option files should not be checked in to source code control. This is also a best practice when working with source code projects and solutions. For example, see [2] an [5].

Avoid pinning of projects to exact versions of TwinCAT 3 Engineering, see [3] and [4]. Always open projects with the most recent version of TwinCAT 3.

Solution

Please update to a recent version of the affected product and uninstall older versions of TwinCAT 3 Engineering. Make sure that older versions of TwinCAT 3 Engineering do not occur as “Remote Manager” versions, see [3]. Remove the “pinning” from your projects to older versions of TwinCAT 3 Engineering, if present, see [4].

Acknowledgement

Beckhoff Automation thanks Peter Cheng from ELEX FEIGONG RESEARCH INSTITUTE of Elex Cybersecurity, Inc. for reporting the issue. 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] Explanation from Microsoft regarding the “Solution User Options (.suo) File”: https://learn.microsoft.com/en-us/visualstudio/extensibility/internals/solution-user-options-dot-suo-file ; accessed 05/19/2025.
[3] Documentation from Beckhoff for the “Remote Manager” feature of TwinCAT 3 Engineering:
https://infosys.beckhoff.com/content/1033/tc3_remote_manager/index.html?id=1584127271344589360
[4] Explanation for “pinning” TwinCAT 3 projects to older versions of TwinCAT 3 Engineering:
https://infosys.beckhoff.com/content/1033/tc3_remote_manager/3154642571.html
[5] Documentation from Beckhoff for “TwinCAT 3 | Source Control” feature of TwinCAT 3 Engineering:
https://infosys.beckhoff.com/content/1033/tc3_sourcecontrol/14604066827.html

History

V 1.0	09/09/2025	Publication