Beckhoff Security Advisory 2024-005:
Local command injection via TwinCAT Package Manager

Publication Date	10/31/2024 (Oct. 31st 2024)
This Update	10/31/2024 (Oct. 31st 2024)
This Version	1.0
Latest Version	PDF
VDE-ID	VDE-2024-064
CVE-ID	CVE-2024-8934
CVSS 3.1	6.5 Medium (AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H)
CVSS 4.0	7.0 High (AV:L/AC:L/AT:N/PR:H/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Weakness Enumerator	CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Summary

A local user with administrative access rights can enter specialy crafted values for settings at the user interface (UI) of the TwinCAT Package Manager which then causes arbitrary OS commands to be executed.

Appearance

Component	**Included in product**	**Affected product version (BEFORE and NOT INCLUDING the named version)**
TwinCAT Package Manager	TwinCAT 3.1 Build 4026	TwinCAT Package Manager setup version < 1.0.603.0

Description

Beckhoff's TwinCAT 3.1 Build 4026 software is modularized and is installed with different packages depending on user requirements. These packages are selected and installed using either the command line utility "tcpkg" or the corresponding graphical user interface called "TwinCAT Package Manager". Both use the same configuration that specifies where to load packages from. These locations are called feeds, have preconfigured default settings and can be customized by administrative users, for example to add another local mirror of a package server. When using the "TwinCAT Package Manager" on a PC, a user with administrative access rights can locally set a specially crafted URL for a feed that causes the TwinCAT Package Manager to execute arbitrary operating system commands.

Mitigation

Administrative users shall always act thoroughly and inspect the values which they enter.

Solution

Please update to a recent version of the affected product.

Acknowledgement

Beckhoff Automation thanks elcazator 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

History

V 1.0	10/31/2024	Publication