BECKHOFF New Automation Technology

Beckhoff Security Advisory 2024-001:
Local authentication bypass in TwinCAT/BSD package “IPC-Diagnostics”

Publication Date	08/27/2024 (Aug 27th 2024)
This Update	08/27/2024 (Aug 27th 2024)
This Version	1.0
Latest Version	PDF
VDE-ID	VDE-2024-045
CVE-ID	CVE-2024-41173
CVSS 3.1	7.8 High (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Weakness Enumerator	CWE-288 Authentication Bypass Using an Alternate Path or Channel

Summary

For TwinCAT/BSD-based products, local users can bypass the authentication mechanism to the device's web interface for the Beckhoff Device Manager and thus gain administrative privileges.

Appearance

Component	Included in product	Affected product version (BEFORE and NOT INCLUDING the named version)
IPC-Diagnostics package	TwinCAT/BSD	IPC-Diagnostics package version < 2.0.0.1
TwinCAT/BSD		TwinCAT/BSD image version < 14.1.2.0_153968

Description

By default, TwinCAT/BSD-based products have a device-specific web interface for web-based management (WBM) enabled, developed by Beckhoff and known as Beckhoff Device Manager UI. It can be accessed remotely or locally. When accessed locally, the authentication mechanism for the web interface can be bypassed by any local user, regardless of their permissions, and they can act with administrative access rights via this mechanism.

Mitigation

Avoid the existence of user accounts with login permission on the target other than administrator access. By default, TwinCAT/BSD has preconfigured user accounts with lower privileges, but none of them have a password, which results in them being denied login access. Avoid running third-party applications on the target that have not been properly audited, regardless of the user they are running as.

Solution

Please update to a recent version of the affected product. In general, Beckhoff recommends updating the entire TwinCAT/BSD operating system to a current version rather than individual packages. Information on updating existing TwinCAT/BSD installations is available in [2]. There you will also find information on how to determine the operating system version via the command line. This is also visible via the Beckhoff Device Manager UI. Please note that when updating from the TwinCAT/BSD major version 12, two consecutive upgrades are required.

Acknowledgement

Beckhoff Automation thanks Andrea Palanca, Nozomi Networks 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
[2] Detailed information on updating the TwinCAT/BSD operating system is provided here:
https://infosys.beckhoff.com/content/1033/twincat_bsd/11780818443.html?id=4222392218353411614

History

V 1.0	08/27/2024	Publication