BECKHOFF New Automation Technology

Beckhoff Security Advisory 2025-003: Vulnerabilities in Beckhoff Device Manager

Publication Date	01/27/2026 (Jan. 27th 2026)
This Update	01/27/2026 (Jan. 27th 2026)
This Version	1.0
Latest Version	PDF
VDE-ID	VDE-2025-092
CVE-ID	CVE-2025-41726
CVSS 3.1	8.8 High (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Weakness Enumerator	CWE-190 Integer Overflow or Wraparound
CVE-ID	CVE-2025-41727
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-420 Unprotected Alternate Channel
CVE-ID	CVE-2025-41728
CVSS 3.1	5.3 Medium (AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)
Weakness Enumerator	CWE-125 Out-of-bounds Read

Summary

CVE-2025-41726: On a Beckhoff IPC or CX device an authenticated user can execute arbitrary code by sending specially crafted calls to the web service of the Beckhoff Device Manager or locally via an API and can cause integer overflows which then can lead to arbitrary code execution within privileged processes.

CVE-2025-41727: On a Beckhoff IPC or CX device a local user can bypass the authentication of the Beckhoff Device Manager user interface, allowing them to perform privileged operations and gain administrator access.

CVE-2025-41728: On a Beckhoff IPC or CX device, an authenticated user may be able to disclose confidential information from the memory of a privileged process by sending specially crafted calls to the Beckhoff Device Manager web service that cause an out-of-bounds read operation and thereby potentially copy confidential information into a response.

Appearance

Component	Affected component version	Included in product
TcPkg Package "Beckhoff.DeviceManager.XAR"	< 2.5.3	IPC / CX with OS Windows 11 IoT Ent. 2024 LTSC
		IPC / CX with OS Windows 10 IoT Ent. 2021 LTSC
		IPC / CX with OS Windows 10 IoT Ent. 2019 LTSC
		IPC / CX with OS Windows 10 IoT Ent. 2016 LTSB
Software "Beckhoff IPC Diagnostics"	< 2.5.3	IPC / CX with OS Windows 11 IoT Ent. 2024 LTSC
		IPC / CX with OS Windows 10 IoT Ent. 2021 LTSC
		IPC / CX with OS Windows 10 IoT Ent. 2019 LTSC
		IPC / CX with OS Windows 10 IoT Ent. 2016 LTSB
Library "MDP.dll"	< 1.7.0.0	IPC / CX with OS Windows Embedded Compact 7
Library "MDP.dll"	< 1.7.0.0	IPC / CX with OS Windows CE 6.0
OS software package "MDP"	< 1.7.0.0	IPC / CX with OS TwinCAT/BSD
OS software package "mdp-bhf"	< 0.0.5-1	IPC / CX with OS Beckhoff RT Linux®

Description

Beckhoff IPC and CX devices are shipped with the Beckhoff Device Manager user interface (UI) installed when they are ordered with an operating system. This Device Manager user interface can be accessed from the network or by a local user. Either way the

user must authenticate before access and have administrative access rights assigned on the device to use the UI. The Beckhoff Device Manager user interface is intended as UI for administrators to configure the device including the creation and maintenance of user accounts and their access rights.

A first vulnerability (CVE-2025-41726, NN-2025-0074) allows an authenticated user (which must have administrative access rights) via network communication to execute arbitrary commands on the device. Therefore the user must inject a specifically crafted message into the communication of the UI with its web service. Also a local user can send a specifically crafted message via an API. In one case the execution of the arbitrary command happens within a privileged process.

A second vulnerability (CVE-2025-41727, NN-2025-0075) allows a local user with low privileges on the device to bypass the authentication mechanism of the UI and send commands to a privileged process which it executes on behalf of that user but with higher privileges. This way the local user can escalate privileges.

A third vulnerability (CVE-2025-41728, NN-2025-0076) allows an authenticated user (which must have administrative access rights) via network communication to cause an out-of-bounds read operation within a specific service process which runs on the device. Therefore the user must inject a specifically crafted message into the communication of the UI with the specific service. The read operation might copy sensitive information from the memory of the specific service into a response message which is then provided to the user but the user cannot choose which information is disclosed.

Mitigation

Beckhoff IPC and CX devices are intended for industrial use within operational technology (OT). For the Beckhoff Device Manager user interface network access is to be restricted to trustworthy personal. Additionally, it is advisable to restrict local access to trustworthy personal.

When not needed, the Beckhoff Device Manager user interface can be disabled for remote access or even be uninstalled. In example, for disabling remote access the OS firewall can be used to forbid the access to the network port or the web server process can be stopped permanently.

Solution

Please update to a recent version of the affected components or update the complete operating system image. Operating system images are available on request from Beckhoff's service (service@beckhoff.com). The setup / installer for Windows 10 and 11 are available on request from Beckhoff's service also.

Acknowledgement

Beckhoff Automation thanks Diego Giubertoni, Nozomi Networks 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	01/27/2026	Publication