BECKHOFF New Automation Technology

Beckhoff Security Advisory 2026-001:
Exposed IOCTLs with insufficient access control in TcRouter.sys

Publication Date	11/11/2026 (Nov. 11th 2026)
This Update	11/11/2026 (Nov. 11th 2026)
This Version	1.0
Latest Version	PDF
VDE-ID	VDE-2026-087
CVE-ID	CVE-2026-18767
CVSS 3.1	7.8 High (AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSS 4.0	8.5 High (AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Weakness Enumerator	CWE-782 Exposed IOCTL with Insufficient Access Control
CVE-ID	CVE-2025-18768
CVSS 3.1	7.8 High (AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSS 4.0	8.5 High (AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Weakness Enumerator	CWE-782 Exposed IOCTL with Insufficient Access Control
CVE-ID	CVE-2025-18769
CVSS 3.1	7.8 High (AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSS 4.0	8.5 High (AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Weakness Enumerator	CWE-782 Exposed IOCTL with Insufficient Access Control

Summary

The vulnerabilities allow local low privileged users or processes to gain full system access on the affected devices through exposed IOCTL function calls.

Appearance

Component	Affected component version	Included in product / component
TC1000 | TwinCAT 3 ADS Build 4024	< 3.1.4024.79	(is the product itself)
TwinCAT 3 | extended Automation Runtime (XAR) Build 4024	< 3.1.4024.79	(is the product itself)
TwinCAT 3 | eXtended Automation Engineering (XAE) Build 4024	< 3.1.4024.79	(is the product itself)
TcPkg Package "TwinCAT.XAR.Base"	< 3.18.1	Product "TwinCAT 3 | Build 4026" for Windows on x64
		Product "TC1000 | TwinCAT ADS" for Windows on x64
		Workload "TwinCAT Standard Runtime" for Windows < 4026.25.0
		Workload "TwinCAT Standard Engineering" for Windows < 4026.25.0
File "TcRouter.sys" for Windows	< 3.1.0.2365	TcPkg Package "TwinCAT.XAR.Base" < 3.18.1
		Product "TC1000 | TwinCAT 3 ADS Build 4024"
		Product "TwinCAT 3 | extended Automation Runtime (XAR) Build 4024
		Product "TwinCAT 3 | eXtended Automation Engineering (XAE) Build 4024"

Description

Some TwinCAT products for Windows operating systems install the driver TcRouter.sys where the affected versions of it expose IOCTL function calls through which a local user or process with SYSTEM privileges can access I/O ports, arbitrary physical memory and move arbitrary physical memory content.

The vulnerability CVE-2026-18767 allows a local low privileged user or process to access I/O ports via TcRouter.sys because of exposed IOCTL function calls resulting in a full compromise of the affected devices.

The vulnerability CVE-2026-18768 allows a local low privileged user to access arbitrary physical memory or define its mapping via TcRouter.sys because of exposed IOCTL function calls resulting in a full compromise of the affected devices.

The vulnerability CVE-2026-18769 allows a local low privileged user can move arbitrary physical memory content via TcRouter.sys because of exposed IOCTL function calls resulting in a full compromise of the affected devices.

Mitigation

Where TwinCAT is installed, dedicate the use of the personal computer to TwinCAT development or programmable logic control and ensure that trustworthy persons have access only and that further software installed there originates from trusted source only. The solution, which is to update to a recent version of the affected components, is the advisable mitigation.

Solution

Please update to a recent version of the affected components.

Acknowledgement

Beckhoff Automation thanks Chi Siang Choo from 4rthur Security Team, Julian Horoszkiewicz from Atos Threat Research Center, and Patrick Saif (alphabetical order) for reporting the issues. 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	11/11/2026	Publication