BECKHOFF New Automation Technology

Beckhoff Security Advisory 2025-002:
XSS Vulnerability in TwinCAT 3 HMI Server

Publication Date	01/20/2026 (Jan. 20th 2026)
This Update	01/20/2026 (Jan. 20th 2026)
This Version	1.0
Latest Version	PDF
VDE-ID	VDE-2025-106
CVE-ID	CVE-2025-41768
CVSS 3.1	5.5 Medium (AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N)
Weakness Enumerator	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Summary

On an instance of TwinCAT 3 HMI Server running on a device an authenticated administrator can inject arbitrary content into the custom CSS field which is persisted on the device and later returned via the login page and error page.

Appearance

Component	Affected component version	Included in product
TcPkg Package "TwinCAT.HMI.Server"	< 14.4.267	TwinCAT 3 XAR for Windows
OS software package "TF2000-HMI-Server"	< 14.4.267	TwinCAT 3 XAR for TwinCAT/BSD
OS software package "tf2000-hmi-server"	< 14.4.267	TwinCAT 3 XAR for Beckhoff RT Linux® on ARM64
OS software package "tf2000-hmi-server"	< 14.4.267	TwinCAT 3 XAR for Beckhoff RT Linux® on AMD64

Description

An optional package of the TwinCAT 3 XAR installs the TwinCAT 3 HMI Server on a device. It provides a server configuration page which can be accessed by administrative users only. When such an administrator accesses the server configuration page it is possible to upload arbitrary content into the CUSTOM_CSS field which is then persisted on the device and later returned and rendered with each login and error page.

Please note that administrators have the access rights to modify any content on the HMI server, for example, via the server configuration page. Therefore, administrators would have to act maliciously to exploit this vulnerability.

Mitigation

Administrators must exercise due diligence when configuring the TwinCAT 3 HMI server via the server configuration page. Administrators must be selected from trustworthy personnel.

Solution

Please update to a recent version of the affected components.

Acknowledgement

Beckhoff Automation thanks Roby Firnando Yusuf, AI Security Lab, Jeonbuk National University 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	01/20/2026	Publication