Siemens Security Advisory by Siemens ProductCERT

SSA-192617: Local Privilege Escalation Vulnerability in TeleControl Server Basic Before V3.1.2.4

Publication Date:	2026-01-13
Last Update:	2026-01-13
Current Version:	V1.0
CVSS v3.1 Base Score:	8.8
CVSS v4.0 Base Score:	7.3

▼ SUMMARY

TeleControl Server Basic before V3.1.2.4 contains a local privilege escalation vulnerability that could allow an attacker to run arbitrary code with elevated privileges.

Siemens has released a new version for TeleControl Server Basic and recommends to update to the latest version.

▼ KNOWN AFFECTED PRODUCTS

Un-/Collapse All

Affected Product and Versions	Remediation
TeleControl Server Basic All versions < V3.1.2.4 affected by CVE-2025-40942	Update to V3.1.2.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109997944/

▼ MITIGATIONS

Product-specific remediations or mitigations can be found in the section Known Affected Products.
Please follow the General Security Recommendations.

▼ GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

▶ PRODUCT DESCRIPTION

▼ VULNERABILITY DESCRIPTION

Un-/Collapse All

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

▼ Vulnerability CVE-2025-40942

Affected application contains a local privilege escalation vulnerability that could allow an attacker to run arbitrary code with elevated privileges.

CVSS v3.1 Base Score	8.8
CVSS v3.1 Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
CVSS v4.0 Base Score	7.3
CVSS v4.0 Vector	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
CWE	CWE-250: Execution with Unnecessary Privileges

▼ ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Peter Cheng from Elex Cybersecurity INC. for reporting the vulnerability

▼ ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT: https://www.siemens.com/cert/advisories

▼ HISTORY DATA

V1.0	(2026-01-13):	Publication Date

▼ TERMS OF USE