Siemens Security Advisory by Siemens ProductCERT

SSA-452276: Eval Injection Vulnerability in SIMATIC S7-1500

Publication Date:	2026-03-10
Last Update:	2026-05-12
Current Version:	V1.3
CVSS v3.1 Base Score:	9.6
CVSS v4.0 Base Score:	9.4

▼ SUMMARY

SIMATIC S7-1500 devices contain a vulnerability that could allow an attacker to inject code by tricking a legitimate user into importing a specially crafted trace file in the web interface.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

▼ KNOWN AFFECTED PRODUCTS

Un-/Collapse All

Affected Product and Versions	Remediation
SIMATIC Drive Controller family	Show more details
SIMATIC ET 200SP Open Controller (incl. SIPLUS variants)	Show more details
SIMATIC S7-1500 CPU family (incl. related ET 200 CPUs and SIPLUS variants)	Show more details
SIMATIC S7-1500 Software Controller	Show more details
SIMATIC S7-PLCSIM Advanced All versions affected by CVE-2025-40943	Currently no fix is available See further recommendations from section Mitigations

▼ MITIGATIONS

Siemens has identified the following specific mitigations that customers can apply to reduce the risk:

- Only upload trusted trace files
- Disable the webserver if not required on the affected systems. Restrict the access to Port 80/tcp and 443/tcp to trusted IP address only

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-2025-40943

Affected devices do not properly sanitize contents of trace files.

This could allow an attacker to inject code through social engineering an authorized user, who has the function right "Read diagnostics", to import a specially crafted trace file.

The malicious trace file is insufficiently sanitized and malicious code could be executed in the clients browser session and trigger PLC operations via the webserver that the legitimate user is authorized to perform.

CVSS v3.1 Base Score	9.6
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
CVSS v4.0 Base Score	9.4
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
CWE	CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')

▼ ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Lukas Sohrmann 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	(2026-03-10):	Publication Date
V1.1	(2026-03-13):	Removed S7-1500 R/H CPU variants as they are not affected by CVE-2025-40943
V1.2	(2026-03-19):	Adjusted title, CVE description enrichment and CWE adjustment
V1.3	(2026-05-12):	Added fix versions for all S7-1500 CPUs that run on firmware version line V2 and V3 and for SIMATIC Drive Controller family. Corrected Simatic ET 200SP Open Controller PC3 family variants

▼ TERMS OF USE

The use of Siemens Security Advisories is subject to the terms and conditions listed on: https://www.siemens.com/productcert/terms-of-use.

 © Siemens 2026