Siemens Security Advisory by Siemens ProductCERT

SSA-981622: Improper Certificate Validation Vulnerability in Siemens Analytics Toolkit

Publication Date:	2026-04-14
Last Update:	2026-04-14
Current Version:	V1.0
CVSS v3.1 Base Score:	3.7
CVSS v4.0 Base Score:	6.3

▼ SUMMARY

Multiple Siemens applications are affected by improper certificate validation in Siemens Analytics Toolkit. This could allow an unauthenticated remote attacker to perform man in the middle attacks.

Siemens has released new versions for the affected products and recommends to update to the latest versions.

▼ KNOWN AFFECTED PRODUCTS

Un-/Collapse All

Affected Product and Versions	Remediation
Siemens Software Center All versions < V3.5.8.2 affected by CVE-2025-40745	Update to V3.5.8.2 or later version https://www.sw.siemens.com/en-US/siemens-software-center/
Simcenter 3D All versions < V2506.6000 affected by CVE-2025-40745	Update to V2506.6000 or later version https://support.sw.siemens.com/product/289054037/
Simcenter Femap All versions < V2506.0002 affected by CVE-2025-40745	Update to V2506.0002 or later version https://support.sw.siemens.com/product/275652363/
Simcenter STAR-CCM+ All versions < V2602 affected by CVE-2025-40745	Update to V2602 or later version https://support.sw.siemens.com/product/226870983/
Solid Edge SE2025 All versions < V225.0 Update 13 affected by CVE-2025-40745	Update to V225.0 Update 13 or later version https://support.sw.siemens.com/product/246738425/
Solid Edge SE2026 All versions < V226.0 Update 04 affected by CVE-2025-40745	Update to V226.0 Update 04 or later version https://support.sw.siemens.com/product/246738425/
Tecnomatix Plant Simulation All versions < V2504.0008 affected by CVE-2025-40745	Update to V2504.0008 or later version https://support.sw.siemens.com/product/297028302/

▼ 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-2025-40745

Affected applications do not properly validate client certificates to connect to Analytics Service endpoint. This could allow an unauthenticated remote attacker to perform man in the middle attacks.

CVSS v3.1 Base Score	3.7
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS v4.0 Base Score	6.3
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CWE	CWE-295: Improper Certificate Validation

▼ ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Konrad Porzezynski 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	(2026-04-14):	Publication Date

▼ TERMS OF USE