Siemens Security Advisory by Siemens ProductCERT

SSA-693776: Multiple Vulnerabilities in Industrial Communication Devices based on SINEC OS before V3.2

Publication Date:	2025-06-10
Last Update:	2026-01-13
Current Version:	V1.1
CVSS v3.1 Base Score:	6.5
CVSS v4.0 Base Score:	7.1

▼ SUMMARY

Several Industrial Communication Devices based on SINEC OS before V3.2 contain multiple vulnerabilities that could allow an attacker to circumvent authorization checks and perform actions that exceed the permissions of the "guest" role.

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
RUGGEDCOM RST2428P (6GK6242-6PA00) All versions < V3.2 ▶ affected by all CVEs	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/
SCALANCE XCM-/XRM-/XCH-/XRH-300 family	Show more details

▼ KNOWN NOT AFFECTED PRODUCTS

Un-/Collapse All

Known Not Affected Products	Reason
SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 family	Show more details

▼ 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-2025-40567

The "Load Rollback" functionality in the web interface of affected products contains an incorrect authorization check vulnerability. This could allow an authenticated remote attacker with "guest" role to make the affected product roll back configuration changes made by privileged users.

CVSS v3.1 Base Score	6.5
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N
CVSS v4.0 Base Score	7.1
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N
CWE	CWE-863: Incorrect Authorization

▼ Vulnerability CVE-2025-40568

An internal session termination functionality in the web interface of affected products contains an incorrect authorization check vulnerability. This could allow an authenticated remote attacker with "guest" role to terminate legitimate users' sessions.

CVSS v3.1 Base Score	4.3
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L
CVSS v4.0 Base Score	5.3
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
CWE	CWE-863: Incorrect Authorization

▼ Vulnerability CVE-2025-40569

The "Load Configuration from Local PC" functionality in the web interface of affected products contains a race condition vulnerability. This could allow an authenticated remote attacker to make the affected product load an attacker controlled configuration instead of the legitimate one. Successful exploitation requires that a legitimate administrator invokes the functionality and the attacker wins the race condition.

CVSS v3.1 Base Score	4.8
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N
CVSS v4.0 Base Score	5.9
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

▼ ADDITIONAL INFORMATION

If the operating system on the device has been changed, please refer to the relevant advisories.

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	(2025-06-10):	Publication Date
V1.1	(2026-01-13):	Corrected SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 family to known not affected.

▼ TERMS OF USE