SSA-083019: Multiple Vulnerabilities in RUGGEDCOM ROS Devices

Publication Date:	2025-07-08
Last Update:	2025-07-08
Current Version:	V1.0
CVSS v3.1 Base Score:	8.8
CVSS v4.0 Base Score:	7.7

SUMMARY

Multiple vulnerabilities affect the RUGGEDCOM Operating System (ROS).

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 countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM ROS V4.X family:	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM i800: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM i801: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM i802: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM i803: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM M2100: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM M2200: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM M969: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM RMC30: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388 V4.X: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RP110: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600F: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600T: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS400: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS401: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416P: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416Pv2 V4.X: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416v2 V4.X: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM RS8000: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000A: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000H: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000T: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900 (32M) V4.X: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900G: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900G (32M) V4.X: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GP: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900L: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-GETS-C01: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-GETS-XX: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900M-STND-C01: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-STND-XX: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900W: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910L: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910W: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS920L: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS920W: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS930L: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS930W: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS940G: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS969: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2100: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100 (32M) V4.X: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100P: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100P (32M) V4.X: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2200: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288 V4.X: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300 V4.X: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300P V4.X: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488 V4.X: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920P V4.X: All versions affected by CVE-2023-52236, CVE-2025-41222, CVE-2025-41223	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS V5.X family:	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See recommendations from section Workarounds and Mitigations

RUGGEDCOM RMC8388 V5.X: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS V5.X NC products:	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388NC V5.X: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416NCv2 V5.X: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416PNCv2 V5.X: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GNC(32M) V5.X: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900NC(32M) V5.X: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100NC(32M) V5.X: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2100PNC (32M) V5.X: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288NC V5.X: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300NC V5.X: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300PNC V5.X: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488NC V5.X: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920PNC V5.X: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSL910NC: All versions < V5.10.0 affected by CVE-2025-41224	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416Pv2 V5.X: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS416v2 V5.X: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900 (32M) V5.X: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900G (32M) V5.X: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100 (32M) V5.X: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100P (32M) V5.X: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288 V5.X: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300 V5.X: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300P V5.X: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2488 V5.X: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG907R: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG908C: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG909R: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG910C: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920P V5.X: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSL910: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST2228: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RST2228P: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST916C: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST916P: All versions < V5.10.0 affected by all CVEs	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations

KNOWN NOT AFFECTED PRODUCTS

Known Not Affected Products	Reason
RUGGEDCOM ROS V4.X family: All versions not affected by CVE-2025-41224	The affected functionality is implemented in a different way and not vulnerable. (Vulnerable Code Not Present)
RUGGEDCOM ROS V4.X NC products: All versions not affected by CVE-2023-52236	The affected features are not supported. (Vulnerable Code Not in Execute Path)
RUGGEDCOM ROS V4.X NC products: All versions not affected by CVE-2025-41222	The affected features are not supported. (Vulnerable Code Not in Execute Path)
RUGGEDCOM ROS V4.X NC products: All versions not affected by CVE-2025-41223	The affected features are not supported. (Vulnerable Code Not in Execute Path)
RUGGEDCOM ROS V5.X NC products: All versions not affected by CVE-2023-52236	The affected features are not supported. (Vulnerable Code Not in Execute Path)
RUGGEDCOM ROS V5.X NC products: All versions not affected by CVE-2025-41222	The affected features are not supported. (Vulnerable Code Not in Execute Path)
RUGGEDCOM ROS V5.X NC products: All versions not affected by CVE-2025-41223	The affected features are not supported. (Vulnerable Code Not in Execute Path)

WORKAROUNDS AND MITIGATIONS

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

- CVE-2023-52236, CVE-2025-41222:
  - Deactivate the SSH server if not required, and if deactivation is supported by the product
  - Deactivate the webserver if not required, and if deactivation is supported by the product
- CVE-2023-52236: Restrict access to port 80/tcp, 443/tcp and 22/tcp to trusted IP addresses only
- CVE-2025-41222: Restrict access to port 80/tcp, 443/tcp and 22/TCP, to trusted IP addresses only
- CVE-2025-41223: Configure the web client to use GCM ciphers; for list of ROS supported cipher suites refer to configuration manual

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

RUGGEDCOM ROS-based devices, typically switches and serial-to-Ethernet devices, are used to connect devices that operate in harsh environments such as electric utility substations and traffic control cabinets.

VULNERABILITY DESCRIPTION

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-2023-52236

The affected products support insecure cryptographic algorithms. An attacker could leverage these legacy algorithms to achieve a man-in-the-middle attack or impersonate communicating parties.

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L
CVSS v4.0 Base Score	6.1
CVSS Vector	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N
CWE	CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Vulnerability CVE-2025-41222

Affected devices do not properly handle malformed TLS handshake messages. This could allow an attacker with network access to the webserver to cause a denial of service resulting in the web server and the device to crash.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
CVSS v4.0 Base Score	6.9
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
CWE	CWE-755: Improper Handling of Exceptional Conditions

Vulnerability CVE-2025-41223

The affected devices support the TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 cipher suite, which uses CBC (Cipher Block Chaining) mode that is known to be vulnerable to timing attacks. This could allow an attacker to compromise the integrity and confidentiality of encrypted communications.

CVSS v3.1 Base Score	4.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v4.0 Base Score	6.3
CVSS Vector	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N
CWE	CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Vulnerability CVE-2025-41224

The affected products do not properly enforce interface access restrictions when changing from management to non-management interface configurations until a system reboot occurs, despite configuration being saved. This could allow an attacker with network access and credentials to gain access to device through non-management and maintain SSH access to the device until reboot.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	7.7
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-693: Protection Mechanism Failure

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 (2025-07-08):	Publication Date

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.