Siemens Security Advisory by Siemens ProductCERT

SSA-912274: Multiple Vulnerabilities in RUGGEDCOM ROX Before V2.17

Publication Date:	2025-12-09
Last Update:	2026-01-13
Current Version:	V1.1
CVSS v3.1 Base Score:	8.8
CVSS v4.0 Base Score:	8.7

▼ SUMMARY

Devices based on RUGGEDCOM ROX before V2.17 contain multiple high severity vulnerabilities.

Siemens has released a new version for RUGGEDCOM ROX II family and recommends to update to the latest version.

▼ KNOWN AFFECTED PRODUCTS

Un-/Collapse All

Affected Product and Versions	Remediation
RUGGEDCOM ROX II 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-2024-56835

The DHCP Server configuration file of the affected products is subject to code injection. An attacker could leverage this vulnerability to spawn a reverse shell and gain root access on the affected system.

CVSS v3.1 Base Score	8.8
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	8.7
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

▼ Vulnerability CVE-2024-56836

During the Dynamic DNS configuration of the affected product it is possible to inject additional configuration parameters. Under certain circumstances, an attacker could leverage this vulnerability to spawn a reverse shell and gain root access on the affected system.

CVSS v3.1 Base Score	7.5
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	7.7
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

▼ Vulnerability CVE-2024-56837

Due to the insufficient validation during the installation and load of certain configuration files of the affected device, an attacker could spawn a reverse shell and gain root access on the affected system.

CVSS v3.1 Base Score	7.2
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	8.6
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

▼ Vulnerability CVE-2024-56838

The SCEP client available in the affected device for secure certificate enrollment lacks validation of multiple fields. An attacker could leverage this scenario to execute arbitrary code as root user.

CVSS v3.1 Base Score	7.2
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	8.6
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

▼ Vulnerability CVE-2024-56839

Code injection can be achieved when the affected device is using VRF (Virtual Routing and Forwarding). An attacker could leverage this scenario to execute arbitrary code as root user.

CVSS v3.1 Base Score	7.2
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	8.6
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE	CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

▼ Vulnerability CVE-2024-56840

Under certain conditions, IPsec may allow code injection in the affected device. An attacker could leverage this scenario to execute arbitrary code as root user.

CVSS v3.1 Base Score	7.2
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	7.5
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

▼ 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	(2025-12-09):	Publication Date
V1.1	(2026-01-13):	Added Children from RUGGEDCOM ROX Family

▼ 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.