SSA-599506: Command Injection Vulnerability in RUGGEDCOM ROX

Publication Date: 2022-07-12
Last Update: 2022-07-12
Current Version: V1.0
CVSS v3.1 Base Score: 7.2

SUMMARY

RUGGEDCOM ROX devices are affected by a command injection vulnerability that could allow an attacker with administrative privileges to gain root access.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM ROX MX5000: All versions < 2.15.1	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/document/109810800 See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX MX5000RE: All versions < 2.15.1	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/document/109810800 See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1400: All versions < 2.15.1	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/document/109810800 See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1500: All versions < 2.15.1	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/document/109810800 See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1501: All versions < 2.15.1	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/document/109810800 See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1510: All versions < 2.15.1	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/document/109810800 See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1511: All versions < 2.15.1	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/document/109810800 See further recommendations from section Workarounds and Mitigations

RUGGEDCOM ROX RX1512: All versions < 2.15.1	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/document/109810800 See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1524: All versions < 2.15.1	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/document/109810800 See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1536: All versions < 2.15.1	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/document/109810800 See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX5000: All versions < 2.15.1	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/document/109810800 See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Apply the principle of least privileges for accounts configured on the affected devices
- Apply Defense-in-Depth practices to the SSH, Web and NETCONF services on ROX

Product specific remediations or mitigations can be found in the section Affected Products and Solution. 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 products provide a level of robustness and reliability that have set the standard for communications networks deployed in harsh environments. Designed to meet and exceed IEC 61850-3 protocol requirements, the RUGGEDCOM Layer 3 Multi-Service Platform family of switches and routers offers integrated router, firewall and VPN functionalities. The RUGGEDCOM RX1400 is a multi-protocol intelligent node which combines Ethernet switching, routing and application hosting capabilities with various wide area connectivity options.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2022-29560

Affected devices do not properly validate user input, making them susceptible to command injection. An attacker with access to either the shell or the web CLI with administrator privileges could access the underlying operating system as the root user.

CVSS v3.1 Base Score	7.2
CVSS 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
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Messner from Siemens Energy 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 (2022-07-12):   Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.