SSA-840800: Code Injection Vulnerability in RUGGEDCOM ROS

Publication Date: 2022-07-12
Last Update: 2022-08-09
Current Version: V1.1
CVSS v3.1 Base Score: 8.0

SUMMARY

RUGGEDCOM ROS-based devices are vulnerable to a web-based code injection attack. To execute this attack, it is necessary to access the system via the Command Line Interface (CLI).

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM ROS i800: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS i801: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS i802: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS i803: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS M969: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS M2100: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS M2200: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RMC30: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RMC8388: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RP110: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM ROS RS400: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS401: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS416: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS416v2: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900 (32M): All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900G: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900G (32M): All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900GP: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900L: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900W: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS910: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS910L: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS910W: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM ROS RS920L: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS920W: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS930L: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS930W: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS940G: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS969: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS1600: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS1600F: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS1600T: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS8000: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS8000A: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS8000H: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS8000T: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG907R: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG908C: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM ROS RSG909R: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG910C: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG920P: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2100: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2100 (32M): All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2100P: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2200: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2288: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2300: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2300P: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2488: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM ROS RSL910: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RST916C: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RST916P: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RST2228: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RST2228P: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/document/109806156/ 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:

- Restrict network access in affected system(s) to ports 443/TCP and 22/TCP, to trusted IP addresses only
- Disable the webserver: Via the Command Line Interface (CLI), go to “Administration”, “Configure IP Services”, “Web Server Users Allowed” and change it to “Disabled” using the keyboard’s up/down arrow keys

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 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 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-2022-34663

Affected devices are vulnerable to a web-based code injection attack via the console.

An attacker could exploit this vulnerability to inject code into the web server and cause malicious behavior in legitimate users accessing certain web resources on the affected device.

CVSS v3.1 Base Score	8.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-94: Improper Control of Generation of Code ('Code Injection')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Aarón Flecha Menéndez and Gabriel Vía Echezarreta from S21Sec 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
V1.1 (2022-08-09):	Added RUGGEDCOM ROS RS1600, RS1600F, RS1600T and RS900 as affected products. Removed RMC, RMC20, RMC40 and RMC41 from affected products. Added new mitigation.

TERMS OF USE