SSA-256353: Third-Party Component Vulnerabilities in RUGGEDCOM ROS

Publication Date: 2022-03-08
Last Update: 2022-04-12
Current Version: V1.2
CVSS v3.1 Base Score: 9.6

SUMMARY

Multiple vulnerabilities affect various third-party components of the RUGGEDCOM ROS, and a cross-site scripting exploit. If exploited, an attacker could cause a denial-of-service, act as a man-in-the-middle or retrieval of sensitive information or gain privileged functions.

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 planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS i801: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS i802: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS i803: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS M969: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS M2100: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS M2200: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RMC: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RMC20: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

RUGGEDCOM ROS RMC30: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RMC40: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RMC41: All versions	Currently no fix is planned 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 planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS400: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS401: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS416: All versions	Currently no fix is planned 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 (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 planned 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 planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900L: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

RUGGEDCOM ROS RS900W: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS910: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS910L: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS910W: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS920L: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS920W: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS930L: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS930W: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS940G: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS969: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS8000: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS8000A: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS8000H: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS8000T: All versions	Currently no fix is planned 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 planned 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 planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2200: All versions	Currently no fix is planned 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 web server access in affected system(s) to ports 443/TCP and 22/TCP, to trusted IP addresses only
- Restrict access to port 69/UDP to trusted IP addresses only, for the TFTP vulnerability

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-2021-37208

Improper neutralization of special characters on the web server configuration page could allow an attacker, in a privileged position, to retrieve sensitive information via cross-site scripting.

CVSS v3.1 Base Score	9.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:H/E:P/RL:T/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2021-42016

A timing attack, in a third-party component, could make the retrieval of the private key possible, used for encryption of sensitive data.

If a threat actor were to exploit this, the data integrity and security could be compromised.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-208: Observable Timing Discrepancy

Vulnerability CVE-2021-42017

A new variant of the POODLE attack has left a third-party component vulnerable due to the implementation flaws of the CBC encryption mode in TLS 1.0 to 1.2.

If an attacker were to exploit this, they could act as a man-in-the-middle and eavesdrop on encrypted communications.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-358: Improperly Implemented Security Check for Standard

Vulnerability CVE-2021-42018

Within a third-party component, whenever memory allocation is requested, the out of bound size is not checked.

Therefore, if size exceeding the expected allocation is assigned, it could allocate a smaller buffer instead. If an attacker were to exploit this, they could cause a heap overflow.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2021-42019

Within a third-party component, the process to allocate partition size fails to check memory boundaries.

Therefore, if a large amount is requested by an attacker, due to an integer-wrap around, it could result in a small size being allocated instead.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2021-42020

The third-party component, in its TFTP functionality fails to check for null terminations in file names.

If an attacker were to exploit this, it could result in data corruption, and possibly a hard-fault of the application.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Messner from Siemens Energy for coordinated disclosure of CVE-2021-37208

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 (2022-03-08):	Publication Date
V1.1 (2022-03-11):	Corrected the list of affected products and fix releases
V1.2 (2022-04-12):	Added acknowledgements

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.