SSA-764417: Weak Encryption Vulnerability in RUGGEDCOM ROS Devices

Publication Date: 2022-03-08
Last Update: 2022-06-14
Current Version: V1.3
CVSS v3.1 Base Score: 6.7

SUMMARY

The SSH server on RUGGEDCOM ROS devices is configured to offer weak ciphers by default. This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over the connection between legitimate clients and the affected device.

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 RMC: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RMC20: 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 RMC40: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RMC41: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RMC8388: All versions	Currently no fix is available See 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	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900 (32M): All versions	Currently no fix is available See 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	Currently no fix is available See 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 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	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG908C: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG909R: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG910C: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG920P: All versions	Currently no fix is available See 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	Currently no fix is available See 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	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2300: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2300P: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2488: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSL910: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RST916C: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RST916P: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RST2228: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RST2228P: All versions	Currently no fix is available See 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:

- Configure the SSH clients to make use of the following strong key exchange ciphers, supported by the ROS SSH server: ecdh-sha2-nistp256, ecdh-sha2-nistp384, or ecdh-sha2-nistp521
- Add only trusted SSH client public keys to ROS and allow access to those clients only

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-2021-37209

The SSH server on affected devices is configured to offer weak ciphers by default.

This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over the connection between legitimate clients and the affected device.

CVSS v3.1 Base Score	6.7
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-326: Inadequate Encryption Strength

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 (2022-03-08):	Publication Date
V1.1 (2022-03-11):	Corrected the list of affected products and fix releases
V1.2 (2022-04-12):	Added acknowledgements
V1.3 (2022-06-14):	Corrected title, vulnerability description, CVSS vector and CWE ID; clarified that a fix release is currently not available for affected devices

TERMS OF USE