SSA-787941: Denial of Service Vulnerability in RUGGEDCOM ROS V4

Publication Date: 2022-11-08
Last Update: 2022-11-08
Current Version: V1.0
CVSS v3.1 Base Score: 5.3

SUMMARY

RUGGEDCOM ROS-based V4 devices are vulnerable to a denial of service attack (Slowloris). By sending partial HTTP requests nonstop, with none completed, the affected web servers will be waiting for the completion of each request, occupying all available HTTP connections. The web server recovers by itself once the attack ends.

Siemens is preparing updates and 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 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS i801 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS i802 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS i803 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RMC30 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RMC8388 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RP110 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS400 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS401 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS416Pv2 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM ROS RS416v2 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900 (32M) V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900G (32M) V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900G V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900GP V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900L V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900M V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS900W V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS910 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS910L V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS910W V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS920L V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS920W V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS930L V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS930W V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM ROS RS940G V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS1600 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS1600F V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS1600T V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS8000 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS8000A V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS8000H V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RS8000T V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG920P V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2100 (32M) V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2100 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2100P V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2200 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2288 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2300 V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS RSG2300P V4.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM ROS RSG2488 V4.X: 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:

- Restrict access to port 80/tcp and 443/tcp to trusted IP addresses only
- Deactivate the webserver if not required, and if deactivation is supported by the product

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-2022-39158

Affected devices improperly handle partial HTTP requests which makes them vulnerable to slowloris attacks.

This could allow a remote attacker to create a denial of service condition that persists until the attack ends.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

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 (2022-11-08): Publication Date

TERMS OF USE