

SSA-459643 Denial of Service Vulnerability in RUGGEDCOM ROS before V5.6.0

Publication Date: 2022-09-13
 Last Update: 2022-09-13
 Current Version: V1.0
 CVSS v3.1 Base Score: 5.3

SUMMARY

RUGGEDCOM ROS-based 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 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 ROS RMC8388: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RS416Pv2: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RS416v2: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RS900 (32M): All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RS900G (32M): All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RSG907R: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RSG908C: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RSG909R: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |

| | |
|---|--|
| RUGGEDCOM ROS RSG910C: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RSG920P: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RSG2100 (32M): All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RSG2288: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RSG2300: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RSG2300P: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RSG2488: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RSL910: All versions < v5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RST916C: All versions < v5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RST916P: All versions < v5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RST2228: All versions < v5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |
| RUGGEDCOM ROS RST2228P: All versions < V5.6.0 | Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ |

WORKAROUNDS AND MITIGATIONS

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-2022-39158

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 (2022-09-13): 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.