SSA-373591: Buffer Overflow Vulnerability in RUGGEDCOM ROS Devices

Publication Date: 2021-07-13
Last Update: 2021-07-13
Current Version: V1.0
CVSS v3.1 Base Score: 8.1

SUMMARY

The latest update for RUGGEDCOM ROS devices fixes a buffer overflow vulnerability in the third party component that could allow an attacker with network access to an affected device to cause a remote code execution condition.

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 i800: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS i801: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS i802: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS i803: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS M969: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS M2100: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS M2200: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RMC: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RMC20: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RMC30: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/

RUGGEDCOM ROS RMC40: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RMC41: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RMC8388 V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RMC8388 V5.X: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RP110: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS400: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS401: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS416: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS416v2 V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS416v2 V5.X: All versions < 5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RS900 (32M) V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS900 (32M) V5.X: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RS900G: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS900G (32M) V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS900G (32M) V5.X: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RS900GP: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/

RUGGEDCOM ROS RS900L: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS900W: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS910: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS910L: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS910W: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS920L: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS920W: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS930L: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS930W: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS940G: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS969: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS8000: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS8000A: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS8000H: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RS8000T: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RSG900 V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/

RUGGEDCOM ROS RSG900 V5.X: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RSG900C: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RSG900G V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RSG900G V5.X: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RSG900R: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RSG920P V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RSG920P V5.X: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RSG2100 (32M) V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RSG2100 (32M) V5.X: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RSG2100 V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RSG2100P: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RSG2100P (32M) V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RSG2100P (32M) V5.X: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RSG2200: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RSG2288 V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RSG2288 V5.X: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/

RUGGEDCOM ROS RSG2300 V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RSG2300 V5.X: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RSG2300P V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RSG2300P V5.X: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RSG2488 V4.X: All versions < V4.3.7	Update to V4.3.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109799880/
RUGGEDCOM ROS RSG2488 V5.X: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RSL910: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RST916C: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RST916P: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/
RUGGEDCOM ROS RST2228: All versions < V5.5.4	Update to V5.5.4 or later version https://support.industry.siemens.com/cs/gb/en/view/109797844/

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Enabling DHCP snooping ensures that the DHCP client in the affected devices will only accept DHCP requests from trusted DHCP servers
- Disable DHCP and configure a static IP address to the device

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-2021-31895

The DHCP client in affected devices fails to properly sanitize incoming DHCP packets. This could allow an unauthenticated remote attacker to cause memory to be overwritten, potentially allowing remote code execution.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

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 (2021-07-13): 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.