SSA-173565: Denial-of-Service Vulnerability in RUGGEDCOM ROX Devices

Publication Date: 2021-10-12
Last Update: 2021-10-12
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

The latest update for RUGGEDCOM ROX devices fixes a vulnerability that could allow an unauthenticated attacker to cause a permanent Denial-of-Service condition under certain conditions.

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 ROX MX5000: All versions < V2.14.1	Update to V2.14.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109800780/
RUGGEDCOM ROX RX1400: All versions < V2.14.1	Update to V2.14.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109800780/
RUGGEDCOM ROX RX1500: All versions < V2.14.1	Update to V2.14.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109800780/
RUGGEDCOM ROX RX1501: All versions < V2.14.1	Update to V2.14.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109800780/
RUGGEDCOM ROX RX1510: All versions < V2.14.1	Update to V2.14.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109800780/
RUGGEDCOM ROX RX1511: All versions < V2.14.1	Update to V2.14.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109800780/
RUGGEDCOM ROX RX1512: All versions < V2.14.1	Update to V2.14.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109800780/
RUGGEDCOM ROX RX1524: All versions < V2.14.1	Update to V2.14.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109800780/
RUGGEDCOM ROX RX1536: All versions < V2.14.1	Update to V2.14.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109800780/
RUGGEDCOM ROX RX5000: All versions < V2.14.1	Update to V2.14.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109800780/

WORKAROUNDS AND MITIGATIONS

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

- Restrict access to the affected systems, especially to port 443/tcp, to trusted IP addresses only

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

ROX-based VPN endpoints and firewall 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-2021-41546

Affected devices write crashdumps without checking if enough space is available on the filesystem. Once the crashdump fills the entire root filesystem, affected devices fail to boot successfully. An attacker can leverage this vulnerability to cause a permanent Denial-of-Service.

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-400: Uncontrolled Resource Consumption

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Communications Security Establishment, CSE for coordinated disclosure
- Loudmouth Security Inc. for coordinated disclosure

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 (2021-10-12): Publication Date

TERMS OF USE