SSA-296266: Denial-of-Service Vulnerability in SCALANCE and RUGGEDCOM Devices

Publication Date: 2021-03-09
Last Update: 2021-04-13
Current Version: V1.1
CVSS v3.1 Base Score: 8.6

SUMMARY

Some firmware versions of the SCALANCE and RUGGEDCOM devices listed below are affected by a vulnerability in the SSH authentication that could allow an attacker to cause a Denial-of-Service under certain conditions.

Siemens has released updates for the affected products and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RM1224: V6.3	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109794349/
SCALANCE M-800: V6.3	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109794349/
SCALANCE S615: V6.3	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109794349/
SCALANCE SC-600: All Versions >= V2.1 and < V2.1.3	Update to V2.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109793041/

WORKAROUNDS AND MITIGATIONS

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

- Configure the built-in firewall to only allow SSH incoming connections from trusted IP addresses

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

The SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C) are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

The SCALANCE M-800 / S615 industrial routers are used for secure remote access to plants via mobile networks, e.g. GPRS or UMTS with the integrated security functions of a firewall for protection against unauthorized access and VPN to protect data transmission.

RUGGEDCOM RM1224 is a 4G ROUTER for wireless IP-communication from Ethernet based devices via LTE(4G)- mobile radio.

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-2021-25676

Multiple failed SSH authentication attempts could trigger a temporary Denial-of-Service under certain conditions. When triggered, the device will reboot automatically.

CVSS v3.1 Base Score	8.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-307: Improper Restriction of Excessive Authentication Attempts

ADDITIONAL INFORMATION

This vulnerability has been discovered internally by Siemens.

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 (2021-03-09): Publication Date
V1.1 (2021-04-13): Added solution for SCALANCE M-800/S615 and RUGGEDCOM RM1224

TERMS OF USE