SSA-451142: Multiple Vulnerabilities in RUGGEDCOM ROX II

Publication Date:	2019-04-09
Last Update:	2019-04-09
Current Version:	V1.0
CVSS v3.0 Base Score:	9.8

SUMMARY

The latest update for RUGGEDCOM ROX II fixes multiple vulnerabilities in third party component software. The most severe vulnerability could allow an attacker to run arbitrary code on the device.

Siemens has released firmware updates for RUGGEDCOM ROX II and recommends that customers update to the new version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM ROX II: All versions < V2.13.0	Update to V2.13.0 The firmware updates for the RUGGEDCOM ROX-based devices can be obtained by contacting the RUGGEDCOM support team at: https://support.industry.siemens.com/my/WW/en/requests#createRequest

WORKAROUNDS AND MITIGATIONS

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

- Disable the BGP routing service if not in use in your setup.
- Configure BGP passwords to authenticate BGP neighbours.

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), 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 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2018-5379

The shipped version of the Quagga BGP daemon (bgpd) can double-free memory when processing certain forms of UPDATE message, containing cluster-list and/or unknown attributes. A successful attack could cause a denial of service or potentially allow an attacker to execute arbitrary code.

The security vulnerability could be exploited by an attacker spoofing a malicious BGP UPDATE message within the network. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality, integrity and availability of the affected system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	9.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-5380

The shipped version of the Quagga BGP daemon (bgpd) can overrun internal BGP code-to-string conversion tables used for debug by 1 pointer value, based on input.

The security vulnerability could be exploited by an attacker spoofing a malicious BGP code-point. Successful exploitation requires the attacker to be in the position of a configured, trusted BGP peer. No system privileges and no user interaction is required. An attacker could use the vulnerability to insert binary data into the internal log files.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	4.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C

Vulnerability CVE-2018-5381

The shipped version of the Quagga BGP daemon (bgpd) has a bug in its parsing of “Capabilities” in BGP OPEN messages. The parser can enter an infinite loop on invalid capabilities causing a denial of service.

The security vulnerability could be exploited by an attacker spoofing a malicious BGP OPEN message. Successful exploitation requires the attacker to be in the position of a configured, trusted BGP peer. No system privileges and no user interaction is required. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the affected system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.5
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

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 (2019-04-09):	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.