

SSA-618620: Vulnerabilities in Boot Loader (U-Boot) of RUGGEDCOM ROS Devices

Publication Date: 2019-12-10
Last Update: 2023-12-12
Current Version: V1.2
CVSS v3.1 Base Score: 7.8

SUMMARY

The boot loader within RUGGEDCOM ROS contains two vulnerabilities in the loading process of the operating system kernel. The more severe of these vulnerabilities could allow an attacker with local access to the device to execute arbitrary code on an affected device.

Siemens recommends specific countermeasures to mitigate this issue.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RMC8388 V4.X: All versions with U-Boot < V2016.05RS09 affected by CVE-2018-18440	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388 V5.X: All versions with U-Boot < V2016.05RS09 affected by CVE-2018-18440	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388NC V4.X: All versions with U-Boot < V2016.05RS09 affected by CVE-2018-18440	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388NC V5.X: All versions with U-Boot < V2016.05RS09 affected by CVE-2018-18440	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG907R: All versions with U-Boot < V2016.05RS09 affected by CVE-2018-18440	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG908C: All versions with U-Boot < V2016.05RS09 affected by CVE-2018-18440	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG909R: All versions with U-Boot < V2016.05RS09 affected by CVE-2018-18440	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG910C: All versions with U-Boot < V2016.05RS09 affected by CVE-2018-18440	Currently no fix is planned See recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG920P V4.X: All versions with U-Boot < V2016.05RS09	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920P V4.X: All versions with U-Boot >= V2016.05RS09 affected by CVE-2019-13103	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920P V5.X: All versions with U-Boot < V2016.05RS09	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920P V5.X: All versions with U-Boot >= V2016.05RS09 affected by CVE-2019-13103	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920PNC V4.X: All versions with U-Boot < V2016.05RS09	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920PNC V4.X: All versions with U-Boot >= V2016.05RS09 affected by CVE-2019-13103	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920PNC V5.X: All versions with U-Boot < V2016.05RS09	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920PNC V5.X: All versions with U-Boot >= V2016.05RS09 affected by CVE-2019-13103	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488 V4.X: All versions with U-Boot < V2016.05RS09	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488 V4.X: All versions with U-Boot >= V2016.05RS09 affected by CVE-2019-13103	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488 V5.X: All versions with U-Boot < V2016.05RS09	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488 V5.X: All versions with U-Boot >= V2016.05RS09 affected by CVE-2019-13103	Currently no fix is planned See recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2488NC V4.X: All versions with U-Boot < V2016.05RS09	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488NC V4.X: All versions with U-Boot >= V2016.05RS09 affected by CVE-2019-13103	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488NC V5.X: All versions with U-Boot < V2016.05RS09	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488NC V5.X: All versions with U-Boot >= V2016.05RS09 affected by CVE-2019-13103	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSL910: All versions with U-Boot < V2016.05RS09 affected by CVE-2018-18440	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSL910NC: All versions with U-Boot < V2016.05RS09 affected by CVE-2018-18440	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RST916C: All versions with U-Boot < V2016.05RS09 affected by CVE-2018-18440	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RST916P: All versions with U-Boot < V2016.05RS09 affected by CVE-2018-18440	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RST2228: All versions with U-Boot < V2016.05RS09	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RST2228: All versions with U-Boot >= V2016.05RS09 affected by CVE-2019-13103	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RST2228P: All versions with U-Boot < V2016.05RS09	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RST2228P: All versions with U-Boot >= V2016.05RS09 affected by CVE-2019-13103	Currently no fix is planned See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Disable boot interface access during boot up via the 'bootoption.txt' file parameter 'Security = yes' to mitigate CVE-2018-18440.
- Disable access to the removable media via 'bootoption.txt' file parameter 'Disableautoaccessremovable = Yes' to mitigate CVE-2019-13103. Note that this vulnerability only applies to RUGGEDCOM ROS, if the device boots from removable media.

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 Ethernet switches are used to operate reliably in electrical harsh and climatically demanding 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-2018-18440

The embedded DENX U-Boot boot loader has a locally exploitable buffer overflow via a crafted kernel image because filesystem loading is mishandled.

The security vulnerability could be exploited by an attacker with local access to the affected systems. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system.

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

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2019-13103

The embedded DENX U-Boot boot loader has a physically exploitable vulnerability. A crafted self-referential DOS partition table will cause the bootloader to infinitely recurse, causing the stack to grow infinitely and eventually crash.

The security vulnerability could be exploited by an attacker with physical access to the affected systems. The vulnerability could allow an attacker to compromise the availability of the system.

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

CVSS v3.1 Base Score 4.6

CVSS Vector [CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C](#)

CWE CWE-674: Uncontrolled Recursion

ADDITIONAL INFORMATION

To check the U-Boot version running on the device consult the respective user manual under section "Accessing the Boot Loader Interface". The version can be extracted by executing the 'version' command in the boot loader interface.

At the time of writing, the boot loader can not be updated on existing devices.

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 (2019-12-10): Publication Date

V1.1 (2022-09-13): Only devices shipped with U-Boot < V2016.05RS09 are affected by CVE-2018-18440, clarify that currently no fix is planned for affected devices

V1.2 (2023-12-12): Removed RUGGEDCOM RSG900C and RSG900R as all products from these families are also listed in the advisory (RUGGEDCOM RSG907R, RSG908C, RSG909R and RSG910C). Readjusted product naming to reflect firmware version used (V4.X or/and V5.X). Added missing products: RUGGEDCOM RMC8388NC, RSG2488NC, RSG920PNC, RST2228P, RST916C and RST916P

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.