SSA-379803: Vulnerabilities in RUGGEDCOM ROX II

Publication Date: 2021-02-09
Last Update: 2021-02-09
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

The latest update for ROX II contains multiple fixes for IPsec related vulnerabilities in Libreswan and NSS.

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 < V2.14.0	Update to V2.14.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109792715/
RUGGEDCOM ROX RX1400: All versions < V2.14.0	Update to V2.14.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109792715/
RUGGEDCOM ROX RX1500: All versions < V2.14.0	Update to V2.14.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109792715/
RUGGEDCOM ROX RX1501: All versions < V2.14.0	Update to V2.14.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109792715/
RUGGEDCOM ROX RX1510: All versions < V2.14.0	Update to V2.14.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109792715/
RUGGEDCOM ROX RX1511: All versions < V2.14.0	Update to V2.14.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109792715/
RUGGEDCOM ROX RX1512: All versions < V2.14.0	Update to V2.14.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109792715/
RUGGEDCOM ROX RX5000: All versions < V2.14.0	Update to V2.14.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109792715/

WORKAROUNDS AND MITIGATIONS

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

- Disable IPsec unless the feature is required in the network environment. Note that IPsec is disabled by default.

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 products provide a level of robustness and reliability that have set the standard for communications networks deployed in harsh environments. Designed to meet and exceed IEC 61850-3 protocol requirements, the RUGGEDCOM Layer 3 Multi-Service Platform family of switches and routers offers integrated router, firewall and VPN functionalities. The RUGGEDCOM RX1400 is a multi-protocol intelligent node which combines Ethernet switching, routing and application hosting capabilities with various wide area connectivity options.

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-2018-12404

A cached side channel attack during handshakes using RSA encryption could allow for the decryption of encrypted content. This is a variant of the Adaptive Chosen Ciphertext attack (AKA Bleichenbacher attack) and affects all NSS versions prior to NSS 3.41.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2018-18508

In Network Security Services (NSS) before 3.36.7 and before 3.41.1, a malformed signature can cause a crash due to a null dereference, resulting in a Denial of Service.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2019-11745

When encrypting with a block cipher, if a call to NSC_EncryptUpdate was made with data smaller than the block size, a small out of bounds write could occur. This could have caused heap corruption and a potentially exploitable crash.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2019-17006

In Network Security Services (NSS) before 3.46, several cryptographic primitives had missing length checks. In cases where the application calling the library did not perform a sanity check on the inputs it could result in a crash due to a buffer overflow.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CWE	CWE-345: Insufficient Verification of Data Authenticity

Vulnerability CVE-2019-17007

In Network Security Services before 3.44, a malformed Netscape Certificate Sequence can cause NSS to crash, resulting in a 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:U/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

Vulnerability CVE-2020-1763

An out-of-bounds buffer read flaw was found in the pluto daemon of libreswan from versions 3.27 till 3.31. An unauthenticated attacker could use this flaw to crash libreswan by sending specially-crafted IKEv1 Informational Exchange packets. The daemon respawns after the crash.

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:U/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

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 (2021-02-09): Publication Date

TERMS OF USE