SSA-406691: Buffer Vulnerabilities in DHCP function of RUGGEDCOM ROX products

Publication Date: 2022-03-08
Last Update: 2022-03-08
Current Version: V1.0
CVSS v3.1 Base Score: 8.8

SUMMARY

A vulnerability in the RUGGEDCOM ROX devices' third party component, ISC DHCP, could allow an attacker to cause a buffer overrun due to a bug when reading a stored DHCP lease containing certain option information, eventually leading to a denial-of-service condition, or cause a remote-code execution.

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 >= V2.3.0 and < V2.15.0	Update to V2.15.0 or later version https://support.industry.siemens.com/cs/document/109805782/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1400: All versions < V2.15.0	Update to V2.15.0 or later version https://support.industry.siemens.com/cs/document/109805782/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1500: All versions >= V2.3.0 and < V2.15.0	Update to V2.15.0 or later version https://support.industry.siemens.com/cs/document/109805782/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1501: All versions >= V2.3.0 and < V2.15.0	Update to V2.15.0 or later version https://support.industry.siemens.com/cs/document/109805782/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1510: All versions >= V2.3.0 and < V2.15.0	Update to V2.15.0 or later version https://support.industry.siemens.com/cs/document/109805782/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1511: All versions >= V2.3.0 and < V2.15.0	Update to V2.15.0 or later version https://support.industry.siemens.com/cs/document/109805782/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM ROX RX1512: All versions >= V2.3.0 and < V2.15.0	Update to V2.15.0 or later version https://support.industry.siemens.com/cs/document/109805782/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1524: All versions < V2.15.0	Update to V2.15.0 or later version https://support.industry.siemens.com/cs/document/109805782/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1536: All versions < V2.15.0	Update to V2.15.0 or later version https://support.industry.siemens.com/cs/document/109805782/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX5000: All versions >= V2.3.0 and < V2.15.0	Update to V2.15.0 or later version https://support.industry.siemens.com/cs/document/109805782/ See further 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 the DHCP server if not needed for operations
- Disable the DHCP client if not needed for operations

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-2021-25217

The affected products contain the third party component, ISC DHCP, that possesses a vulnerability if used as a DHCP client or server. The vulnerability affects the DHCP package when storing and reading DHCP lease information containing particular option information.

An attacker could exploit this vulnerability to affect the availability of the DHCP client or server, or in the worst case affect the confidentiality or integrity of device through a buffer overflow or cause a remote-code execution.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

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 (2022-03-08): Publication Date

TERMS OF USE