SSA-189842: TCP URGENT/11 Vulnerabilities in RUGGEDCOM Win

Publication Date: 2019-09-10
Last Update: 2019-12-10
Current Version: V1.1
CVSS v3.1 Base Score: 9.8

SUMMARY

RUGGEDCOM Win is affected by multiple security vulnerabilities. These vulnerabilities could allow an attacker to leverage various attacks, e.g. to execute arbitrary code over the network.

The vulnerabilities affect the underlying Wind River VxWorks network stack and were recently patched by Wind River.

Siemens is working on updates for the affected products, and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM WIN70xx Base Station: All versions < BS5.2.461.17	Update to BS5.2.4624.17 https://support.industry.siemens.com/cs/ww/en/view/109773083
RUGGEDCOM WIN72xx Base Station: All versions < BS5.2.461.17	Update to BS5.2.4624.17 https://support.industry.siemens.com/cs/ww/en/view/109773083

WORKAROUNDS AND MITIGATIONS

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

- Block TCP traffic to the IP address of the management interface

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 WIN products are used as base stations or subscriber units in wide area private wireless networks. The products are compliant to the IEEE 802.16e standard and can be operated in harsh environments.

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-2019-12255

By sending specially crafted TCP packets with a manipulated TCP Urgent Pointer to a device, an attacker could potentially execute arbitrary code. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

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:P/RL:O/RC:C
CWE	CWE-191: Integer Underflow (Wrap or Wraparound)

Vulnerability CVE-2019-12256

By sending IPv4 packets with specially crafted IP options to a device, an attacker could potentially execute arbitrary code. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

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:P/RL:O/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2019-12257

By sending specially crafted DHCP packets to a device, an attacker could potentially execute arbitrary code. Adjacent network access, but no authentication and no user interaction is needed to conduct this attack.

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

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-12258

By sending TCP packets with specially crafted TCP options to a device, an attacker could potentially trigger a Denial-of-Service (DoS) condition. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

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:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2019-12259

By sending specially crafted IGMP packets to a device, an attacker could potentially trigger a Denial-of-Service (DoS) condition. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

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:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2019-12260

By sending specially crafted TCP packets with a manipulated TCP Urgent Pointer to a device, an attacker could potentially execute arbitrary code. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

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:P/RL:O/RC:C
CWE	CWE-371: State Issues

Vulnerability CVE-2019-12261

While connecting to a remote host, specially crafted TCP packets with a manipulated TCP Urgent Pointer could potentially cause the execution of arbitrary code on the device. It is required that the affected device connects to a malicious system to conduct this attack.

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

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:P/RL:O/RC:C
CWE	CWE-191: Integer Underflow (Wrap or Wraparound)

Vulnerability CVE-2019-12262

By sending unsolicited reverse ARP packets to a device, an attacker may be able to affect availability and integrity of the device. Adjacent network access, but no authentication and no user interaction is needed to conduct this attack.

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

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-840: Business Logic Errors

Vulnerability CVE-2019-12263

By sending specially crafted TCP packets with a manipulated TCP Urgent Pointer to a device, an attacker could potentially trigger a race condition and potentially execute arbitrary code. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2019-12264

By sending specially crafted DHCP packets to a device, an attacker may be able to affect availability and integrity of the device. Adjacent network access, but no authentication and no user interaction is needed to conduct this attack.

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

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-840: Business Logic Errors

Vulnerability CVE-2019-12265

By sending specially crafted IGMPv3 packets to a device, an attacker may be able to obtain a limited amount of data from the device. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-840: Business Logic Errors

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 (2019-09-10): Publication Date
V1.1 (2019-12-10): Added updates for RUGGEDCOM WIN70xx Base Station and RUGGEDCOM WIN72xx Base Station

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.