SSA-560465: DHCP Client Vulnerability in VxWorks-based Industrial Products

Publication Date:	2021-07-13
Last Update:	2021-07-13
Current Version:	V1.0
CVSS v3.1 Base Score:	9.8

SUMMARY

Various industry products are affected by a DHCP client vulnerability in Wind River VxWorks, that could allow an attacker to cause a heap-based buffer overflow.

Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM WIN Subscriber Station: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X200-4 P IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT PRO: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X202-2 IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X202-2P IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X202-2P IRT PRO: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X204 IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X204 IRT PRO: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X204-2 (incl. SIPLUS NET variant): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X204-2FM: All versions	See recommendations from section Workarounds and Mitigations

SCALANCE X204-2LD (incl. SIPLUS NET variant): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X204-2LD TS: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X204-2TS: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X206-1: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X206-1LD: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X208: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X208 PRO: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X212-2: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X212-2LD: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X216: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X224: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X300/X408 family (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF201-3P IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF202-2P IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF204: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF204 IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF204-2: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF204-2BA IRT: All versions	See recommendations from section Workarounds and Mitigations

SCALANCE XF206-1: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF208: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF 181 EIP: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF 182C: All versions	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:

- Avoid the use of the DHCP client if unnecessary to your environment.
- If the DHCP client is enabled, it is recommended to disable it.

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.

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

SIMATIC RF181EIP

SIMATIC RF182C is an RFID communication module for direct connection of SIMATIC identification systems to Ethernet/IP. SIMATIC RF182C is superseded by the SIMATIC RF18xC devices (RF185C, RF186C, RF188C).

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

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-2021-29998

There is a DHCP vulnerability in Wind River VxWorks, for versions prior to 6.5. The vulnerability could cause a possible heap overflow if exploited.

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:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

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 (2021-07-13):	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.