SSA-181018: Heap Overflow Vulnerability in SCALANCE X switches, RUGGEDCOM Win, RFID 181EIP, and SIMATIC RF182C

Publication Date: 2018-06-12
Last Update: 2020-12-08
Current Version: V1.6
CVSS v3.1 Base Score: 7.5

SUMMARY

SCALANCE X switches, RUGGEDCOM Win, RFID 181EIP, and SIMATIC RF182C are affected by a vulnerability that could allow an unprivileged attacker located in the same local network segment (OSI Layer 2) to gain system privileges by sending a specially crafted DHCP response to a client's DHCP request.

Siemens has released updates for several affected products and recommends to update to the new versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RFID 181EIP: All versions	See recommendations from section Workarounds and Mitigations
RUGGEDCOM Win: V4.4, V4.5, V5.0, and V5.1	Update to V5.2 https://support.industry.siemens.com/cs/ww/en/view/109762466
SCALANCE X-200 switch family (incl. SIPLUS NET variants): All versions < V5.2.3	Update to V5.2.3 https://support.industry.siemens.com/cs/ww/en/view/109758142
SCALANCE X-200IRT switch family (incl. SIPLUS NET variants): All versions < V5.4.1	Update to V5.4.1 https://support.industry.siemens.com/cs/ww/en/view/109758144
SCALANCE X-200RNA switch family: All versions < V3.2.6	Update to V3.2.6 https://support.industry.siemens.com/cs/ww/en/view/109767359
SCALANCE X-300 switch family (incl. SIPLUS NET variants): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547
SCALANCE X408: All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547
SCALANCE X414: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF182C: All versions	See recommendations from section Workarounds and Mitigations

 © Siemens 2020

WORKAROUNDS AND MITIGATIONS

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

- Use static IP addresses instead of DHCP
- Apply cell protection concept: https://www.siemens.com/cert/operational-guidelines-industrial-security
- Apply Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security
- For SIMATIC RF182C and RFID 181EIP: migrate to a successor product within the SIMATIC RF18xC/CI family, V1.3 or later version. For details refer to the phase-out announcement.

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

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

The SCALANCE X-204RNA Industrial Ethernet network access points enable the cost-effective connection of non-PRP terminal devices to separate parallel networks, where a high availability is required.

RUGGEDCOM Win

RFID 181EIP is an RFID communication module for direct connection of SIMATIC identification systems to Ethernet/IP. RFID 181EIP is superseded by the SIMATIC RF18xC devices (RF185C, RF186C, RF188C).

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).

SIMATIC RF185C, RF186C/CI, and RF188C/CI are communication modules for direct connection of SIMATIC identification systems to PROFINET IO/Ethernet and OPC UA.

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/.

 © Siemens 2020

Vulnerability CVE-2018-4833

Unprivileged remote attackers located in the same local network segment (OSI Layer 2) could gain remote code execution on the affected products by sending a specially crafted DHCP response to a client's DHCP request.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Dr. Ang Cui and Joseph Pantoga from Red Balloon Security for coordinated disclosure
- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2018-06-12):	Publication Date
V1.1 (2018-12-11):	Added solution for RUGGEDCOM Win
V1.2 (2018-12-13):	Update for RUGGEDCOM Win not available, see mitigations
V1.3 (2019-01-08):	Added solution for RUGGEDCOM Win
V1.4 (2019-06-11):	Clarified product names. Added solution for SCALANCE X200RNA
V1.5 (2020-01-14):	SIPLUS devices now explicitly mentioned in the list of affected products. Added patch information for SCALANCE X-300 switch family (incl. SIPLUS NET variants) and SCALANCE X408.
V1.6 (2020-12-08):	Informed about successor products for SIMATIC RF182C and RFID 181EIP

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.