SSA-344983: Vulnerability in WPA2 Key Handling affecting SCALANCE W700 and SCALANCE W1700 Devices

Publication Date:	2019-12-10
Last Update:	2019-12-10
Current Version:	V1.0
CVSS v3.1 Base Score:	6.5

SUMMARY

The latest firmware updates for the SCALANCE W700 and W1700 wireless device families fix a vulnerability affecting WPA/WPA2 key handling. It might be possible to, by manipulating the EAPOL-Key frames, decrypt the Key Data field without the frame being authenticated.

This has impact on WPA/WPA2 architectures using TKIP encryption. The attacker must be in the wireless range of the device to perform the attack.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1700: All versions < V1.1	Update to V1.1 or any later version https://support.industry.siemens.com/cs/ww/en/view/109762253
SCALANCE W700: All versions < V6.4	Update to V6.4 or any later version https://support.industry.siemens.com/cs/ww/en/view/109773308

WORKAROUNDS AND MITIGATIONS

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

- Whenever possible, use AES-CCMP instead of TKIP in the WPA/WPA2 networks. This can be configured for both SCALANCE W-700 and W-1700 families over the Web Based Management (web server). For more information, go for the respective Manual.

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 W700 products are wireless communication devices used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

SCALANCE W1700 products are wireless communication devices used to connect industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs), according to the IEEE 802.11ac standard.

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-2018-14526

It was discovered that under certain conditions the integrity of EAPOL-key messages might not be checked, leading to a decryption oracle.

The security vulnerability could be exploited by an attacker within range of the Access Point which could allow the abuse of the vulnerability to access confidential data. For this, the Access Point must use TKIP as encryption method.

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

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C
CWE	CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel

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 (2019-12-10):	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.