SSA-901333: KRACK Attacks Vulnerabilities in Industrial Products

Publication Date: 2017-11-09
Last Update: 2018-11-13
Current Version: V1.5
CVSS v3.0 Base Score: 6.8

SUMMARY

Multiple vulnerabilities affecting WPA/WPA2 implementations were identified by a researcher and publicly disclosed under the term "Key Reinstallation Attacks" (KRACK). These vulnerabilities could potentially allow an attacker within the radio range of the wireless network to decrypt, replay or inject forged network packets into the wireless communication.

Several Siemens Industrial products use WPA/WPA2 and are therefore affected by some of the vulnerabilities.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RS9xxW: All versions	See recommendations from section Workarounds and Mitigations
RUGGEDCOM RX1400 with WLAN interface: All versions < V2.11.2	Install V2.11.2 The firmware updates for the RUGGEDCOM ROX-based devices can be obtained by contacting the RUGGEDCOM support team at: https://support.industry.siemens.com/my/WW/en/requests#createRequest
SCALANCE W-700 (IEEE 802.11a/b/g): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE W-700 (IEEE 802.11n): All versions < V6.2.1	Install V6.2.1 or newer https://support.industry.siemens.com/cs/us/en/ps/21965/dl
SCALANCE W1750D: All versions < V6.5.1.5-4.3.1.8	Install V6.5.1.5-4.3.1.8 https://support.industry.siemens.com/cs/ww/en/view/109756771
SCALANCE WLC711: All versions < V9.21.19.003	Install V9.21.19.003 https://support.industry.siemens.com/cs/ww/en/view/109755170
SCALANCE WLC712: All versions < V9.21.19.003	Install V9.21.19.003 https://support.industry.siemens.com/cs/ww/en/view/109755170
SIMATIC ET200 PRO IM154-6 PN IWLAN: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IWLAN-PB/LINK: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC Mobile Panel 277(F) IWLAN: All versions	See recommendations from section Workarounds and Mitigations
SINAMICS V20 Smart Access Module: 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:

- The attacker must be within radio range of the affected devices. The attacker must trigger the start of a new WLAN handshake in order to perform the attack. If WPA2- CCMP (AES) is configured on the devices, then attacks are limited to decryption and replay of parts of the network traffic. The attacker cannot join the Wireless network, or obtain the WPA2 key.
- SCALANCE WLC711 and WLC712 are only affected by the vulnerabilities related to the group key in the default configuration. An attacker is therefore not able to access unicast traffic. The devices are only affected by CVE-2017-13082 if they have 802.11r functionality activated. IEEE 802.11r is deactivated by default. The devices are only affected by the remaining vulnerabilities if the functions “MeshConnex” or “Client Bridge Mode” are active. Both functions are disabled by default. If these modes have been activated and are not required for the operation of a wireless environment, then customers can deactivate the functionality to reduce the risk.
- SCALANCE W-700 devices that are operated in Client mode, SIMATIC Mobile Panel 277F IWLAN, and SIMATIC ET200 WLAN are not affected if the iPCF, iPCF-MC, or iPCF-HT features are enabled.
- SCALANCE W-700 devices operated in Access Point mode are only affected if WDS with WPA2 encryption is configured. If iPCF, iPCF-MC, or iPCF-HT is active on all interfaces, then SCALANCE W-700 devices are not vulnerable.
- RUGGEDCOM RX1400 and RS9xxW are not vulnerable if operated in Access Point mode.
- SCALANCE W1750D devices are not vulnerable to these vulnerabilities in the default configuration. Only customers that enabled the “Mesh” or “WiFi uplink” functionality are affected by the vulnerabilities. Disabling these functionalities will completely mitigate the vulnerabilities.
- Ensure multiple layers of security, do not depend on the security of WPA2 alone.
- Use WPA2-CCMP (AES) instead of WPA2-TKIP or WPA-GCMP, if supported by the WLAN clients to reduce the risk of potential attacks
- Apply Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to run the devices in a protected IT environment, Siemens particularly 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 Ethernet switches and ROX-based VPN endpoints and firewalls with fiber optic WAN options integrate an IEEE 802.11b/g Wireless Access Point/Client/Bridge and are used to operate reliably in electrical harsh and climatically demanding environments such as electric utility substations and traffic control cabinets.

SCALANCE W-700 products are wireless communication devices which offer reliability, ruggedness and security for both non-critical communication and process-critical data. The devices are used where mobility of machines and parts is required, or cable installation is too expensive or difficult to implement.

The SCALANCE W1750D controller-based Direct Access Points support radio transmission according to the latest IWLAN standard IEEE 802.11ac Wave 2.

SCALANCE WLC711 and WLC712 controllers allow simple management of industrial wireless networks.

SIMATIC ET 200 PRO IM154-6 PN IWLAN Interface modules for PROFINET IO are used to connect ET200 PRO field devices (IO Devices) to controllers (IO Controller) via PROFINET.

SIMATIC IWLAN-PB/LINK devices allow network transition between industrial WLAN and Profibus with PROFINET IO functionality.

SIMATIC Mobile Panel 277(F) IWLAN is designed for HMI tasks of medium complexity for wireless use in PROFINET environments.

SINAMICS V20 Smart Access is a Web server module that can be easily mounted onto the SINAMICS V20 drives family to execute commissioning, service- and maintenance tasks.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability (CVE-2017-13077)

Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the pairwise key in the four-way handshake.

CVSS v3.0 Base Score	4.2
CVSS Vector	CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C

Vulnerability (CVE-2017-13078)

Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group TemporalKey (GTK) during the four-way handshake, allowing an attacker within radio range to replay frames from access points to clients.

CVSS v3.0 Base Score	4.2
CVSS Vector	CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C

Vulnerability (CVE-2017-13079)

Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11w allows reinstallation of the Integrity Group Temporal Key (IGTK) during the four-way handshake, allowing an attacker within radio range to spoof frames from access points to clients.

CVSS v3.0 Base Score	5.9
CVSS Vector	CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N/E:P/RL:O/RC:C

Vulnerability (CVE-2017-13080)

Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group TemporalKey (GTK) during the group key handshake, allowing an attacker within radio range to replay frames from access points to clients.

CVSS v3.0 Base Score	4.2
CVSS Vector	CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C

Vulnerability (CVE-2017-13081)

Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11w allows reinstallation of the Integrity Group Temporal Key (IGTK) during the group keyhandshake, allowing an attacker within radio range to spoof frames from access points to clients.

CVSS v3.0 Base Score	4.2
CVSS Vector	CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C

Vulnerability (CVE-2017-13082)

Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11r allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the fast BSS transmission (FT) handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.

CVSS v3.0 Base Score	6.8
CVSS Vector	CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

Vulnerability (CVE-2017-13084)

Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Station-To-Station Link(STSL) Transient Key (STK) during the PeerKey handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.

CVSS v3.0 Base Score	6.8
CVSS Vector	CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

Vulnerability (CVE-2017-13086)

Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Tunnelled Direct Link Setup (TDLS) Peer Key (TPK) during the TDLS handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.

CVSS v3.0 Base Score	6.8
CVSS Vector	CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

Vulnerability (CVE-2017-13087)

Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation ofthe Group Temporal Key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients.

CVSS v3.0 Base Score	4.2
CVSS Vector	CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C

Vulnerability (CVE-2017-13088)

Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Integrity Group Temporal Key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients.

CVSS v3.0 Base Score	4.2
CVSS Vector	CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C

ADDITIONAL INFORMATION

Further information on the vulnerabilities by the researcher: https://www.krackattacks.com

For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2017-11-09):	Publication Date
V1.1 (2017-12-05):	Clarified mitigating factors; added update information for SCALANCEW700 (IEEE 802.11n)
V1.2 (2017-12-18):	Added upate information for RUGGEDCOM RX1400 with WLAN
V1.3 (2018-01-24):	New advisory format; added update information for WLC711 and WLC712
V1.4 (2018-04-05):	Added update information for SCALANCE W1750D
V1.5 (2018-11-13):	Changed update information for SCALANCE W-700 (IEEE 802.11n)

TERMS OF USE