SSA-418456: KRACK Attacks Vulnerabilities in SIMATIC RF350M and SIMATIC RF650M

Publication Date 2017-12-18
Last Update 2017-12-18
Current Version V1.0
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) [2]. 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.

Siemens released a driver update for SIMATIC RF350M and SIMATIC RF650M, which fixes these vulnerabilities. Siemens recommends applying the driver update.

AFFECTED PRODUCTS

- SIMATIC RF350M: All versions with Summit Client Utility < V22.3.5.16
- SIMATIC RF650M: All versions with Summit Client Utility < V22.3.5.16

DESCRIPTION

SIMATIC RF350M and SIMATIC RF650M expand the RF300 and RF600 RFID systems with a powerful mobile RFID reader for applications in the areas of production and service. In addition, it is an aid for startup and testing.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2017-13077)

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

CVSS Base Score 6.8

Vulnerability 2 (CVE-2017-13078)

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

CVSS Base Score 4.2

Vulnerability 3 (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 Base Score 5.9
Vulnerability 4 (CVE-2017-13080)
Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the group key handshake, allowing an attacker within radio range to replay frames from access points to clients.

CVSS Base Score 4.2

Vulnerability 5 (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 key handshake, allowing an attacker within radio range to spoof frames from access points to clients.

CVSS Base Score 4.2

Mitigating Factors
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.

SOLUTION
Siemens provides driver update V22.3.5.16 [1] for SIMATIC RF350M and SIMATIC RF650M, which fixes the vulnerabilities.

It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES
[1] Driver update V22.3.5.16 for SIMATIC RF350M and SIMATIC RF650M can be obtained from:
[2] Description of the vulnerabilities by the researcher:
https://www.krackattacks.com/
https://www.siemens.com/cert/operational-guidelines-industrial-security
[4] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity
[5] 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 (2017-12-18): Publication Date

DISCLAIMER
See: https://www.siemens.com/terms_of_use