SSA-712518: Information Disclosure Vulnerability (Kr00k) in Industrial Wi-Fi Products

Publication Date: 2020-08-11
Last Update: 2020-08-11
Current Version: V1.0
CVSS v3.1 Base Score: 3.1

SUMMARY

An information disclosure vulnerability (CVE-2019-15126, also known as Kr00k) could allow an attacker to read a discrete set of traffic over the air after a Wi-Fi device state change.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC RF350M: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF650M: All versions	See recommendations from section Workarounds and Mitigations
SIMOTICS CONNECT 400: 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:

- SIMATIC RF350M and RF650M: Disable Wi-Fi if possible
- SIMOTICS CONNECT 400: No specific countermeasures needed as the data is protected via TLS on application layer

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

SIMATIC RFx50M are handheld RFID reader/writer terminals with application software for customizing RFID tags.

SIMOTICS CONNECT 400 is a connector and sensor box, mounted on low-voltage motors to provide analytics data for the MindSphere application SIDRIVE IQ Fleet.

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-2019-15126

An issue was discovered on Broadcom Wi-Fi client devices. Specifically timed and handcrafted traffic can cause internal errors (related to state transitions) in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic.

CVSS v3.1 Base Score	3.1
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

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 (2020-08-11): 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.