SSA-516174: Wi-Fi Encryption Bypass Vulnerabilities in SCALANCE W1750D

Publication Date: 2023-05-09
Last Update: 2023-10-10
Current Version: V1.1
CVSS v3.1 Base Score: 8.4

SUMMARY

The SCALANCE W1750D device is affected by Wi-Fi encryption bypass vulnerabilities ("Framing Frames") that could allow an attacker to disclose sensitive information or to steal the victims session.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1750D (JP) (6GK5750-2HX01-1AD0): All versions < V8.10.0.6	Update to V8.10.0.6 or later version The update is available upon request from customer support
SCALANCE W1750D (ROW) (6GK5750-2HX01-1AA0): All versions < V8.10.0.6	Update to V8.10.0.6 or later version The update is available upon request from customer support
SCALANCE W1750D (USA) (6GK5750-2HX01-1AB0): All versions < V8.10.0.6	Update to V8.10.0.6 or later version The update is available upon request from customer support

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution.
Please follow the General Security Recommendations.

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 W1750D is an Access Point that supports IEEE 802.11ac standards for high-performance WLAN, and is equipped with two dual-band radios, which can provide access and monitor the network simultaneously.

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-2022-47522

The IEEE 802.11 specifications through 802.11ax allow physically proximate attackers to intercept (possibly cleartext) target-destined frames by spoofing a target's MAC address, sending Power Save frames to the access point, and then sending other frames to the access point (such as authentication frames or re-association frames) to remove the target's original security context. This behavior occurs because the specifications do not require an access point to purge its transmit queue before removing a client's pairwise encryption key.

CVSS v3.1 Base Score	8.4
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/E:F/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

ADDITIONAL INFORMATION

Siemens SCALANCE W1750D is a brand-labeled device from Aruba.
Aruba separates the listed vulnerability in 3 scenarios:
Scenario 1 “Exploiting Power Save Features": The affected products are not vulnerable to this scenario.
Scenario 2 “Security Context Override (SCO)": The affected products are vulnerable to this scenario and there is no fix available.
Scenario 3 “Fast Reconnect Attack": The affected products are vulnerable to this scenario and the fix version listed in this advisory fixes this scenario.

For more information regarding the listed vulnerability and its scenarios see the Aruba security advisory ARUBA-PSA-2023-005 (https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-005.txt) and the original published paper (https://papers.mathyvanhoef.com/usenix2023-wifi.pdf).

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 (2023-05-09):	Publication Date
V1.1 (2023-10-10):	Added fix for SCALANCE W1750D family

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.