SSA-913875: Frame Aggregation and Fragmentation Vulnerabilities in 802.11

Publication Date: 2021-07-13
Last Update: 2021-07-13
Current Version: V1.0
CVSS v3.1 Base Score: 6.5

SUMMARY

Twelve vulnerabilities in the implementation of frame aggregation and fragmentation of the 802.11 standard, under the name of FragAttacks, have been published.

Successful exploitation of these vulnerabilities could allow an attacker within Wi-Fi range to forge encrypted frames, which could result in sensitive data disclosure and possibly traffic manipulation.

The advised Siemens products are only affected by some of the published vulnerabilities.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W700 IEEE 802.11ax: All versions only affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146	See recommendations from section Workarounds and Mitigations
SCALANCE W700 IEEE 802.11n: All versions only affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	See recommendations from section Workarounds and Mitigations
SCALANCE W1700 IEEE 802.11ac: All versions only affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26146, CVE-2020-26147	See recommendations from section Workarounds and Mitigations
SCALANCE W1750D: All versions only affected by CVE-2020-24588, CVE-2020-26146	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:

- As these vulnerabilities can only be exploited within Wi-Fi range, when possible reduce Wi-Fi transmission power or make sure to have the devices in private areas with physical access controls

- When possible, A-MSDU can be disabled to mitigate CVE-2020-24588 and CVE-2020-26144

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 based on IEEE 802.11 standards. They are used to connect all to sorts of WLAN devices (Access Points or Clients, depending on the operating mode) with a strong focus on industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs) and others.

SCALANCE W1700 products are wireless communication devices based on IEEE 802.11 standards. They are used to connect all to sorts of WLAN devices (Access Points or Clients, depending on the operating mode) with a strong focus on industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs) and others.

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

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-2020-26147

An issue was discovered in the Linux kernel 5.8.9. The WEP, WPA, WPA2, and WPA3 implementations reassemble fragments even though some of them were sent in plaintext. This vulnerability can be abused to inject packets and/or exfiltrate selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:N/E:U/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-26146

An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WPA, WPA2, and WPA3 implementations reassemble fragments with non-consecutive packet numbers. An adversary can abuse this to exfiltrate selected fragments. This vulnerability is exploitable when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used. Note that WEP is vulnerable to this attack by design.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-26145

An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WEP, WPA, WPA2, and WPA3 implementations accept second (or subsequent) broadcast fragments even when sent in plaintext and process them as full unfragmented frames. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-26144

An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WEP, WPA, WPA2, and WPA3 implementations accept plaintext A-MSDU frames as long as the first 8 bytes correspond to a valid RFC1042 (i.e., LLC/SNAP) header for EAPOL. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-26143

An issue was discovered in the ALFA Windows 10 driver 1030.36.604 for AWUS036ACH. The WEP, WPA, WPA2, and WPA3 implementations accept fragmented plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-26141

An issue was discovered in the ALFA Windows 10 driver 6.1316.1209 for AWUS036H. The Wi-Fi implementation does not verify the Message Integrity Check (authenticity) of fragmented TKIP frames. An adversary can abuse this to inject and possibly decrypt packets in WPA or WPA2 networks that support the TKIP data-confidentiality protocol.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:U/RC:C
CWE	CWE-354: Improper Validation of Integrity Check Value

Vulnerability CVE-2020-26140

An issue was discovered in the ALFA Windows 10 driver 6.1316.1209 for AWUS036H. The WEP, WPA, WPA2, and WPA3 implementations accept plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:U/RC:C
CWE	CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

Vulnerability CVE-2020-26139

An issue was discovered in the kernel in NetBSD 7.1. An Access Point (AP) forwards EAPOL frames to other clients even though the sender has not yet successfully authenticated to the AP. This might be abused in projected Wi-Fi networks to launch denial-of-service attacks against connected clients and makes it easier to exploit other vulnerabilities in connected clients.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2020-24588

The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SSP A-MSDU frames (which is mandatory as part of 802.11n), an adversary can abuse this to inject arbitrary network packets.

CVSS v3.1 Base Score	3.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:U/RL:U/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

ADDITIONAL INFORMATION

For more details regarding the FragAttacks vulnerabilities refer to:

- Fragment and Forge Breaking Wi-Fi Through Frame Aggregation and Fragmentation: https://papers.mathyvanhoef.com/usenix2021.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 (2021-07-13): Publication Date

TERMS OF USE