Alcatel·Lucent Enterprise

ALE Security Advisory No. SA-N0095 Ed. 01

802.11 Frame Aggregation and Fragmentation Vulnerabilities

Summary

Twelve new vulnerabilities related to different components in the implementation of the 802.11 standard have been published. Successful exploitation of each one of these vulnerabilities can result in sensitive data disclosure and possibly traffic manipulation.

CVEs

CVE-2020-24586, CVE-2020-24587, CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26142, CVE-2020-26143, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146, CVE-2020-26147

Description of Issue

Vulnerabilities in the implementation of the IEEE 802.11 standard have been uncovered. These vulnerabilities allow an attacker to inject malicious frames in a legitimate Wi-Fi connection, regardless of the type of wireless encryption used. Successful exploitation of these vulnerabilities results in exfiltration of sensitive data or, in conjunction with other known attacks, allows for traffic manipulation. Note that these vulnerabilities might also affect wireless client devices. Non-AOS-W devices may also have fixes for these vulnerabilities. Please check with your non-AOS-W device vendor for additional details.

1. Accepting non-SPP A-MSDU frames (CVE-2020-24588)

The 802.11 standard allows for encryption of the data payload, but the MAC header remains unencrypted. To cryptographically protect the header fields, it requires a WLAN device to compute additional authentication data (AAD) using some of these header fields. The AAD is used for MIC computation as part of CCMP encryption. The AAD does not include the A-MSDU Present bit from the QoS Control subfield of the 802.11 MAC header by default. The bit is included in AAD only if the capabilities advertised by the Access Point and the client devices include support and mandate for signal and payload protected (SPP) A-MSDU aggregation, as against the default payload protected (PP) A-MSDU aggregation.

By using a MitM (Machine-in-the-Middle) technique and altering the A-MSDU bit from the QoS Control subfield of the 802.11 MAC header, an attacker can have access to sensitive data and/or inject data to the victim.

Internal reference: ATLWL-219
Severity: MEDIUM
CVSSv3 Overall Score: 6.1
CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N

2. Reassembling encrypted fragments with non-consecutive packet numbers (CVE-2020-26146)

The 802.11 standard allows for fragmentation of data frames that are larger than a particular value (known as the fragmentation threshold) into more than one MPDU for transmission over the air. On the receiving device, these fragments are then reassembled into the original data frame and passed to the higher layers of the stack. The MAC header includes a Sequence Number (SN) subfield for ordering of the MPDUs irrespective of whether they contain fragmented or unfragmented data. To facilitate fragmentation, the MAC header also includes a Fragment Number (FN) subfield in addition SN – fragments of one data frame have the same SN but different FN. Once encrypted, the MPDUs also have a Packet Number (PN) which is again a consecutively increasing number used for checking against replays. Together, PN are expected to increase linearly with FN and SN.

The AOS-W Access Point does not check whether all fragments of a frame have consecutive PN, that is, whether the fragments indeed belong to the same frame or not. Consequently, the attacker using a MitM (Machine-in-the-Middle) technique can abuse this vulnerability by mixing fragments of different packets in order to extract user data.

Internal reference: ATLWL-220
Severity: MEDIUM
CVSSv3 Overall Score: 4.7
CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Status on Alcatel-Lucent Enterprise AOS-W Products

List of products and releases concerned (or affected):

Product Name	Release
AOS-W Instant Access points affected by CVE-2020-24588 and CVE-2020-26146.	AOS-W Instant 6.4.x: prior to 6.4.4.8-4.2.4.19 AOS-W Instant 6.5.x: prior to 6.5.4.19 - prior to 6.5.4.20 if using IAP-1xx series AOS-W Instant 8.3.x: prior to 8.3.0.15 - prior to 8.3.0.16 if using RAP-155 series AOS-W Instant 8.5.x: prior to 8.5.0.12 - prior to 8.5.0.13 if using RAP-155 series AOS-W Instant 8.6.x: prior to 8.6.0.8 - prior to 8.6.0.9 if using RAP-155 series AOS-W Instant 8.7.x: prior to 8.7.1.2 All AOS-W Access Points when managed by hardware or virtual implementations of AOS-W Mobility Controllers: AOS-W 6.4.x: prior to 6.4.4.25 AOS-W 6.5.x: prior to 6.5.4.19 - prior to 6.5.4.20 if using AP-1xx series AOS-W 8.3.x: prior to 8.3.0.15 - prior to 8.3.0.16 if using AP-1xx series AOS-W 8.5.x: prior to 8.5.0.12 - prior to 8.5.0.13 if using AP-1xx series AOS-W 8.6.x: prior to 8.6.0.8 - prior to 8.6.0.9 if using AP-1xx series AOS-W 8.7.x: prior to 8.7.1.2
ALE views these vulnerabilities as Medium severity. Other AOS-W products not listed above, including AOS-W Mobility Conductor (formerly Mobility Master) are not affected by these vulnerabilities.	

List of products and releases **NOT concerned** (or affected):

Product Name	Release
All AOS-W products are not affected by: CVE-2020-24586, CVE-2020-24587, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26142, CVE-2020-26143, CVE-2020-26144, CVE-2020-26145, CVE-	All releases.

2020-26147	

Workarounds

None.

Resolution for Alcatel-Lucent Enterprise Affected Products

Upgrade software per the following recommendations, as applicable:

AOS-W Instant Access Points:

- AOS-W Instant 6.4.x: 6.4.4.8-4.2.4.19 and above
- AOS-W Instant 6.5.x: 6.5.4.19 and above
    - 6.5.4.20 and above if using IAP-1xx series
- AOS-W Instant 8.3.x: 8.3.0.15 and above
    - 8.3.0.16 and above if using RAP-155 series
- AOS-W Instant 8.5.x: 8.5.0.12 and above
    - 8.5.0.13 if using RAP-155 series
- AOS-W Instant 8.6.x: 8.6.0.8 and above
    - 8.6.0.9 and above if using RAP-155 series
- AOS-W Instant 8.7.x: 8.7.1.2 and above
- AOS-W Instant 8.8.x: 8.8.0.0 and above

Access Points when managed by hardware or virtual implementations of AOS-W Mobility Controllers:

- AOS-W 6.4.x: 6.4.4.25 and above
- AOS-W 6.5.x: 6.5.4.19 and above
    - 6.5.4.20 and above if using AP-1xx series
- AOS-W 8.3.x: 8.3.0.15 and above
    - 8.3.0.16 and above if using AP-1xx series
- AOS-W 8.5.x: 8.5.0.12 and above
    - 8.5.0.13 and above if using AP-1xx series
- AOS-W 8.6.x: 8.6.0.8 and above
    - 8.6.0.9 and above if using AP-1xx series
- AOS-W 8.7.x: 8.7.1.2 and above
- AOS-W 8.8.x: 8.8.0.0 and above

History

Ed.01 (2021 May 11th): creation