

ALE Security Advisory **No. SA-N0050** **Ed. 01**

AOS-W - WPA2 Key Reinstallation Vulnerabilities

Summary

Common industry-wide flaws in WPA2 key management may allow an attacker to decrypt, replay, and forge some frames on a WPA2 encrypted network. The accompanying FAQ document provides more extensive details.

Description of Issue

See the accompanying FAQ document published by Aruba for more detailed information.

Reinstallation of the pairwise key in the 4-way handshake (CVE-2017-13077)

Reinstallation of the group key in the 4-way handshake (CVE-2017-13078)

Reinstallation of the integrity group key in the 4-way handshake (CVE-2017-13079)

Reinstallation of the group key in the group key handshake (CVE-2017-13080)

Reinstallation of the integrity group key in the group key handshake (CVE-2017-13081)

AOS-W and AOS-W Instant are not affected by the above vulnerabilities while acting as an authenticator (i.e. operating in standard AP mode).

AOS-W APs are affected by the above vulnerabilities while acting as a Wi-Fi supplicant in the following modes:

- Mesh

AOS-W Instant is affected by the above vulnerabilities while acting as a Wi-Fi supplicant in the following modes:

- Mesh
- Wi-Fi Uplink

Severity: Medium

CVSSv3 Overall Score: 6.7

CVSS Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Accepting a retransmitted FT Reassociation Request (CVE-2017-13082)

AOS-W and AOS-W Instant are affected by this vulnerability in both authenticator and supplicant modes.

Severity: Medium

CVSSv3 Overall Score: 6.7

CVSS Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Reinstallation of the STK key in the PeerKey handshake (CVE-2017-13084)

Reinstallation of the Tunneled Direct-Link Setup PeerKey (CVE-2017-13086)

Reinstallation of the Group Key when processing a WNM Sleep Mode Response (CVE-2017-13087)

Reinstallation of the Integrity Group Key when processing a WNM Sleep Mode Response (CVE-2017-13088)

AOS-W products are not affected by these vulnerabilities.

Status on Alcatel-Lucent Enterprise WLAN Products

List of products and releases concerned (or affected):

Product Name	Release
AOS-W	<ul style="list-style-type: none"> - AOS-W (all versions prior to 6.3.1.25) - AOS-W 6.4 prior to 6.4.4.16 - AOS-W 6.5.0.x - AOS-W 6.5.1 prior to 6.5.1.9 - AOS-W 6.5.2.x - AOS-W 6.5.3 prior to 6.5.3.3 - AOS-W 6.5.4 prior to 6.5.4.2 - AOS-W 8.x prior to 8.1.0.4 - AOS-W Instant (all versions prior to 4.2.4.9) - AOS-W Instant 4.3 prior to 4.3.1.6 - AOS-W Instant 6.5.2 and 6.5.3 prior to 6.5.3.3 - AOS-W Instant 6.5.4 prior to 6.5.4.2

FIPS and non-FIPS versions of software are both affected equally.

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

Product Name	Release
No other AOS-W products are affected	N/A

Workarounds

All vulnerabilities described in this advisory may be mitigated by disabling certain features:

- For AOS-W, ensure that 802.11r is disabled by verifying that any configured SSID profile does not contain a "dot11r-profile". From the command line, "show wlan dot11r-profile" will list any 802.11r profiles that have been configured. If the reference count is 0, 802.11r is not enabled.
- For AOS-W Instant, ensure that 802.11r is not enabled in any configured WLAN.
- Disabling 802.11r on the AP infrastructure will effectively mitigate client-side 802.11r vulnerabilities. It will not, however, mitigate client-side 4-way handshake vulnerabilities.
- Mesh mode for both AOS-W and AOS-W Instant is vulnerable. Until this vulnerability is patched, mesh networks should be disabled.
- Wi-Fi uplink mode for AOS-W Instant is vulnerable. Until this vulnerability is patched, the Wi-Fi uplink feature should not be used.

Resolution for Alcatel-Lucent Enterprise Affected Products

All listed vulnerabilities have been fixed in the following AOS-W patch releases, which are available for download immediately from support.esd.alcatel-lucent.com:

- 6.3.1.25
- 6.4.4.16
- 6.5.1.9
- 6.5.3.3
- 6.5.4.2
- 8.1.0.4

All listed vulnerabilities have been fixed in the following AOS-W Instant patch releases, which are available for download immediately:

- 4.2.4.9
- 4.3.1.6
- 6.5.3.3
- 6.5.4.2

History

Ed.01 (2017 October 16th): creation