# WPA2/WPA Key Reinstall Vulnerabilities

Modified on: Mon, 16 Oct, 2017 at 2:01 AM

Several vulnerabilities have been disclosed today regarding WPA2/WPA implementation in WiFi clients and APs. Mojo Networks has already provided remediation for these vulnerabilities. See below for actions you need to take to mitigate them in your network environment.

| CVE Numbers | Fix to Address Root Cause | Mitigation till Fix | WIPS Zero Day Protection |
|---|---|---|---|
| CVE-2017-13077<br>CVE-2017-13078<br>CVE-2017-13079<br>CVE-2017-13080<br>CVE-2017-13081<br>CVE-2017-13087<br>CVE-2017-13088 | Update Client Software | Update Mojo AP software to 8.5. This version is already loaded in the Mojo cloud. However, network owners need to upgrade their APs to version 8.5. On-premise server customers need to download the 8.5 software bundle from the support portal and upgrade their devices.<br><br>For C-50, C-55, C-60 and O-70 devices, this fix will be available by upgrading devices to version 8.2.1-902.25. This version is already loaded in the Mojo cloud for relevant platforms. For on-premise servers, this version is packaged in 8.5 bundle available on support portal.<br><br>After device upgrades are complete, network owners need to check select the checkbox labelled as “Mitigate WPA2/WPA key reinstallation vulnerabilities in clients” in the Wi-Fi Profile menu. Mitigation is recommended only until clients are patched and is not a permanent solution. This is because, in a small percent of cases, mitigation can interfere with client connectivity.<br><br>Please note that this mitigation is applicable to all the 7 listed CVEs even though the bulb text mentions only 5 CVEs. Two new CVEs were published after the product build. | These CVEs require AP MAC spoofing for exploitation. Full time Mojo WIPS (not the background scanning WIPS one) can block AP MAC spoofing if corresponding prevention policy is enabled. Full time Mojo WIPS can block AP MAC spoofing of any WLAN AP that it protects. If C130 third radio is being used for full time WIPS, then it does not protect MAC spoofing of the same C130 device, but protects MAC spoofing of the adjacent C130 device. |

| CVE Numbers | Fix to Address Root Cause | Mitigation till Fix | WIPS Zero Day Protection |
|---|---|---|---|
| CVE-2017-13082 | This is fixed in Mojo AP software release 8.5 (802.11ac platforms) and 8.2.1-902.25 (11n platforms) | None | None |
| CVE-2017-13084<br>CVE-2017-13086 | Update client software | Mojo AP customers may enable “Client Isolation” feature in Wi-Fi profile to block these vulnerabilities. These vulnerabilities will not show up in typical enterprise networks. They pertain to case where clients connected to the same AP set up peer to peer session among themselves with the AP’s help. | These require AP MAC spoofing for exploitation, hence full time Mojo WIPS can block them as explained above. |

**NOTE**:

- Both 802.1x (EAP) and PSK (password) based networks are affected by all 10 of these CVEs.
- Both WPA2 Only and Mixed Mode (WPA2/WPA) are affected by all 10 of these CVEs.