# Sierra Wireless Technical Bulletin: WPA Vulnerabilities

## Products: Sierra Wireless GX400,GX440,GX450,MP70,oMG500,oMG2000, MG90, FX30/30S 3G, WP76/77xx,WPx5xx,AR8652,AR755x, AR758x, AR759x

Date of issue: 6 March 2019

Recently published research has identified several vulnerabilities in the Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) standard. The following Common Vulnerability and Exposure (CVE) identifiers have been assigned to each of the vulnerabilities:

- CVE-2017-13077: reinstallation of the pairwise key in the Four-way handshake
- CVE-2017-13078: reinstallation of the group key in the Four-way handshake
- CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake
- CVE-2017-13080: reinstallation of the group key in the Group Key handshake
- CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake
- CVE-2017-13082: accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pairwise key while processing it
- CVE-2017-13084: reinstallation of the STK key in the PeerKey handshake
- CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake
- CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
- CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

Sierra Wireless would like to thank Mathy Vanhoef and Frank Piessens of the imec-DistriNet research group of KU Leuven for discovering and responsibly reporting this issue, as well as the efforts of CERT and ICASI for coordinating the response. For more information please refer to the links below:

- https://papers.mathyvanhoef.com/ccs2017.pdf
- http://www.icasi.org/wi-fi-protected-access-wpa-vulnerabilities
- https://www.kb.cert.org/vuls/id/228519

## Scope of Impact

The CVEs reported above affect 3 different modes of Wi-Fi operation when used in conjunction with WPA or WPA2 security:

- Peer-to-Peer or “Adhoc” networking:
  - CVE-2017-13084
  - CVE-2017-13086
- Access Point operation, specifically when the Fast Transition option is enabled (AP with FT)
  - CVE-2017-13082
- Client operation
  - CVE-2017-13077
  - CVE-2017-13078
  - CVE-2017-13079
  - CVE-2017-13080
  - CVE-2017-13081
  - CVE-2017-13087
  - CVE-2017-13088

## Affected Products

The following table lists the product impacts of the three groups of vulnerabilities listed above and the current state of remediation planning. This bulletin will be updated when firmware update release dates are finalized. Please visit https://sierrawireless.com/security for the latest information.

| Product | Vulnerability Impact | | | Fix Version | Target Release Date |
|---|---|---|---|---|---|
| | AdHoc | Access Point | Client | | |
| GX400/440[1] | N/A | **NOT** Affected | Affected | 4.4.9 | Q4 2019 |
| GX450[1] | N/A | **NOT** Affected | Affected | 4.9.4 | Released Feb 15, 2019 |
| MP70 | N/A | **NOT** Affected | Affected | ALEOS 4.9 | Released Dec 27, 2017 |
| oMG500/2000 | N/A | **NOT** Affected | Affected | MGOS 3.14.6 | Released Oct 25, 2017 |
| MG90 | N/A | **NOT** Affected | Affected | MGOS 4.1.2 | Released Dec 18, 2017 |
| FX30/30S 3G[2] | Affected [4] | Affected [4] | Affected [4] | FW Release 15 | Released July 2018 |
| WP76/77xx[3] | Affected [4] | Affected [4] | Affected [4] | FW Release 7 | Released Dec 29, 2017 |
| WPx5xx[3] | Affected [4] | Affected [4] | Affected [4] | FW Release 15 | Released Dec 11, 2017 |
| AR755x[3],AR8652 | Affected [4] | Affected [4] | Affected [4] | TBD | TBD |
| AR758x[3] | Affected[4] | Affected[4] | Affected[4] | SWI9x28A_00.11.04.00+ | Released Nov 2017 |
| AR759x[3] | Affected[4] | Affected[4] | Affected[4] | SWI9x40A_01.12.05.00+ | Released Nov 2017 |

[1]When equipped with a Wi-Fi X-Card

[2]When equipped with a Wi-Fi IoT Card

[3]When configured to manage a Wi-Fi radio

[4]If configured to operate in this mode

## Mitigation Options

If you are using affected device functions, the best mitigation until the required firmware updates can be applied is to encrypt data traversing the vulnerable Wi-Fi link with a VPN or application-layer encryption. If this is not possible users should evaluate the sensitivity of data transferred over the Wi-Fi connection and consider disabling the vulnerable functions until a firmware update can be applied.

Customers using AR8652 or AR755x products to manage Wi-Fi connectivity have the option to install the latest hostapd/wpa_supplicant patches if they need to update their products before the next firmware update is released.

## Further Information

For further information and technical support, please contact your Sierra Wireless representative. To contact Sierra Wireless, please visit https://www.sierrawireless.com/company/contact-us/.