Product Security Advisory: Aggregation and Fragmentation Attacks

Sierra Wireless Advisory: SWI-PSA-2021-003 (link to latest version)

Date: May 11, 2021

Summary

Recently published research has identified various design flaw vulnerabilities in the Wi-Fi standard and vulnerabilities in Wi-Fi implementations. The following Common Vulnerabilities and Exposure (CVE) identifiers have been assigned to each of the vulnerabilities:

CVE-ID	Description
CVE-2020-24586	Not clearing fragments from memory when (re)connecting to a network.
CVE-2020-24587	Reassembling fragments encrypted under different keys.
CVE-2020-24588	Accepting non-SPP A-MSDU frames.
CVE-2020-26139	Forwarding EAPOL frames even though the sender is not yet authenticated.
CVE-2020-26140	Accepting plaintext data frames in a protected network.
CVE-2020-26141	Not verifying the TKIP MIC of fragmented frames.
CVE-2020-26142	Processing fragmented frames as full frames.
CVE-2020-26143	Accepting fragmented plaintext data frames in a protected network.
CVE-2020-26144	Accepting plaintext A-MSDU frames that start with an RFC1042 header with EtherType EAPOL (in an encrypted network).
CVE-2020-26145	Accepting plaintext broadcast fragments as full frames (in an encrypted network).
CVE-2020-26146	Reassembling encrypted fragments with non-consecutive packet numbers.
CVE-2020-26147	Reassembling mixed encrypted/plaintext fragments.

Affected Products

The following AirLink products are affected:

Product(s)	Affected Version(s)	Planned Fix Date
XR90	< AirLink OS 2.1	Q3 2021
MP70 and MP70E	All ALEOS versions	To be announced
RV55, LX40 and LX60	< ALEOS 4.16	Q3 2021
GX450	All ALEOS versions	No fix planned
OMG2000	All MGOS versions	No fix planned
MG90	All MGOS versions	To be announced

The following AirPrime products are affected:

Product(s)	Affected Version(s)	Planned Fix Date
WP75xx	< FW R17	No fix planned
WP76xx	< FW R17	Q4 2021
WP77xx	< FW R15	Q2 2022
WP85xx	< FW R17	No fix planned
BX3105	< FW R2.73	Q2 2022

Recommended Actions

Sierra Wireless recommends upgrading to the latest release versions for your products as soon as they become available.

Credits

Sierra Wireless would like to thank Mathy Vanhoef (New York University Abu Dhabi) for discovering and responsibly reporting these issues, as well as the efforts of ICASI and the Wi-Fi Alliance for coordinating the response. For more information please refer to the links below:

https://fragattacks.com

https://www.wi-fi.org/security-update-fragmentation

https://www.icasi.org/aggregation-fragmentation-attacks-against-wifi/

Support Contact Information

Sierra Wireless Technical Support is available by phone or web portal from 6:00 to 17:00 PST, Monday to Friday.
Phone (Toll Free): 1-877-687-7795
Web: https://www.sierrawireless.com/support/community-portal/

Security Bulletins

To see the latest security updates from Sierra Wireless, please visit:
https://www.sierrawireless.com/company/security/