Product Security Advisory: AMM Unauthenticated Login

Sierra Wireless Advisory SWI-PSA-2020-007 (link to latest version)

Date of issue: November 19, 2020

Summary

Internal security testing by Sierra Wireless has uncovered a vulnerability in AMM session handling that allows an unauthenticated user to login with administrator privileges.

Affected Products

All AMM versions prior to 2.17 are impacted.

Scope of Impact

A session handling flaw in the AMM user interface allows an unauthenticated user to login with administrator privileges.

CVE-2020-11101 has been assigned to this vulnerability. Sierra Wireless has assigned a CVSSv3 score of 9.8 (Critical) to this vulnerability based on the vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Recommended Actions

Sierra Wireless recommends upgrading AMM to version 2.17 immediately to address this vulnerability. All hosted AMM instances have been upgraded to version 2.17. Sierra Wireless has contacted customers with publicly-reachable AMM instances to encourage them to upgrade.

Pending upgrade, network access to the AMM should be restricted via network and firewall configuration. This may include:

- Removing access to the AMM via public IP addresses. If users outside of a trusted domain must connect to the AMM, a VPN architecture can be used.
- Limiting access to the AMM via the Restricted IP option. Please contact Sierra Wireless Technical Support for assistance in configuring this option.

Note that, even with network and firewall controls, low-privileged users who can connect to the AMM can still use this vulnerability to gain administrator privileges.

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/