Product Security Advisory: MGOS Security Update

Sierra Wireless Advisory SWI-PSA-2020-006 (link to latest version)

Date of issue: November 19, 2020

Summary

Sierra Wireless has confirmed two security issues in MGOS that were reported by external parties.

Affected Products

The issues impact the following AirLink products and versions:

- oMG2000 running MGOS 3.15.1 or earlier
- MG90 running MGOS 4.2.1 or earlier

Both issues are fixed in MGOS 3.15.2 and MGOS 4.3.

Scope of Impact

MGOS Forced Browsing

A locally connected, unauthenticated user can read log files that contain sensitive system information.

CVE-2019-13988 has been assigned to this issue, with the title “MGOS Forced Browsing.” Sierra Wireless has assigned a CVSSv3.0 score of 8.8 (High) based on the vector CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

MGOS Command Injection

A command injection is possible through the user interface, allowing arbitrary command execution as the root user.

CVE-2020-13712 has been assigned to this issue, with the title “MGOS Command Injection.” Sierra Wireless has assigned a CVSSv3.0 score of 7.8 (High) based on the vector CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H.

Recommended Actions

Sierra Wireless recommends upgrading to the latest MGOS version for your gateway.

For devices that cannot be upgraded, Sierra Wireless recommends that customers control access to the Wi-Fi and Ethernet interfaces of the device.

Credits

CVE-2019-13988 “MGOS Forced Browsing” was independently reported by New York City Cyber Command and another researcher.

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/