Sierra Wireless Technical Bulletin: Brute Force Threat

Date of Issue: February 11, 2019

Applicable Products:

AirLink® oMG2000 and oMG500 routers with MGOS 3.15.1 or older firmware, and MG90 routers with MGOS 4.1.2 or older firmware, that are directly reachable from the public internet.

Introduction

The Sierra Wireless security team has discovered a new brute force intrusion threat on oMG2000, oMG500 and MG90 routers that have the SSH port 2222 directly reachable from the public internet. Upon investigation, this appears to be a non-targeted attack and part of a wider global campaign on port 2222 across various devices on the internet. We take such threats seriously and are actively working with our partners and customers to address the threat and assist in remediation of affected routers.

To date, we have only seen evidence of unsuccessful brute force login attempts on the SSH port. However, in some cases, high concentration of login attempts can drive high CPU usage resulting in device reboots and can also lead to higher data charges.

While Sierra Wireless cannot control incoming connection requests, following the recommended actions will prevent the router from responding to such requests which will protect the router from threat of brute force password attacks and can aid in reducing data overages. All customers are advised to immediately take action as detailed in this bulletin.

Recommended Actions

Sierra Wireless advises customers to follow the recommended actions outlined below. If you require assistance performing these actions or have routers that are exhibiting suspicious behavior, please contact your authorized AirLink reseller and/or your Sierra Wireless sales or technical representative. Alternatively, you can also contact Sierra Wireless technical support for assistance.

Device	Recommended Action
MG90 with MGOS 4.1.2 or older firmware	Upgrade to the latest firmware MGOS 4.2.2. (MGOS 4.2.0 firmware restricted access to the SSH port.)
oMG2000 and oMG500 with MGOS 3.15.1 or older firmware	Update the firewall rule as per the steps detailed below.

Note: If you've enabled the SSH ports post MGOS 4.2.0, or have custom enabled ports other than port 2222 over the WAN, please take the necessary steps to disable these ports or contact Sierra Wireless for assistance.

To update the firewall rule for oMG2000 and oMG500 routers:

1. Navigate to Advanced Routing Rules in the LCI, and add or update the '**WAN-Device State Change**' rule (refer to Section 11.8 of the oMG Software Configuration Guide for more information).
2. Add the following script to the rule:

```
# Disable ssh port access
if [ "$2" == "up" ] ; then
 /sbin/iptables -D INPUT -i $1 -p tcp --dport 22 -j DROP &> /dev/null
 /sbin/iptables -I INPUT 1 -i $1 -p tcp --dport 22 -j DROP
 /sbin/iptables -D INPUT -i $1 -p tcp --dport 2222 -j DROP &> /dev/null
 /sbin/iptables -I INPUT 1 -i $1 -p tcp --dport 2222 -j DROP
fi
```

   Note: oMG devices running older versions of MGOS may still have SSH available on port 22; while we have not yet observed increased attacks on this port, the recommended script also closes this port as a precautionary measure.

3. Reboot the device.

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:portal.sierrawireless.com