Airspan web UI private keys and config files in webroot

Low vladionescu published GHSA-9v93-3qpc-hxj9 on Jul 20

Package

AirVelocity 1500 eNB (Airspan)

Affected versions

9.3.0.01249, 15.18.00.2511

Patched versions

None

Description

Vulnerability Description

An authenticated attacker can enumerate and download sensitive files, including the UI's TLS private key, the web server binary, and the web server configuration file.

Proof of Concept

Accessing `https://<device>/bin/` in the web UI after authenticating results in a listing of files that includes the private key (`mini_httpd.pem`), the mini_httpd config file (`web.conf`), and the web server binary itself (`mini_httpd`).

Fix

Airspan released version 15.18.00.2511 in early June which partially fixed this issue by disabling directory listings, but the files are still accessible at their direct URLs.

Timeline

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

Severity

Low

CVE ID

CVE-2022-36306

Weaknesses

CWE-219 CWE-548

Credits

 tchebb

 vladionescu