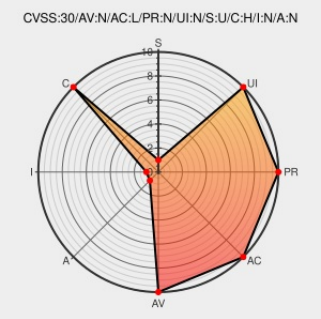
CVE-2017-9136

Published on: 05/21/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:56 PM UTC

CVE-2017-9136

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Backhaul Radios from Mimosa contain the following vulnerability:

An issue was discovered on Mimosa Client Radios before 2.2.3. In the device's web interface, there is a page that allows an attacker to use an unsanitized GET parameter to download files from the device as the root user. The attacker can download any file from the device's filesystem. This can be used to view unsalted, MD5-hashed administrator passwords, which can then be cracked, giving the attacker full admin access to the device's web interface. This vulnerability can also be used to view the plaintext pre-shared key (PSK) for encrypted wireless connections, or to view the device's serial number (which allows an attacker to factory reset the device).

CVE-2017-9136 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	NONE	NONE

CVE References

Description	Tags	Link
404 — Page not found	Third Party Advisory blog.iancaling.com text/html Inactive Link Not Archived	MISC blog.iancaling.com/post/160596244178

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Mimosa	Backhaul Radios	All	All	All	All
Operating System	Mimosa	Client Radios	All	All	All	All

cpe:2.3:o:mimosa:backhaul_radios:*:*:*:*:*:*:*:*:

cpe:2.3:o:mimosa:client_radios:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→