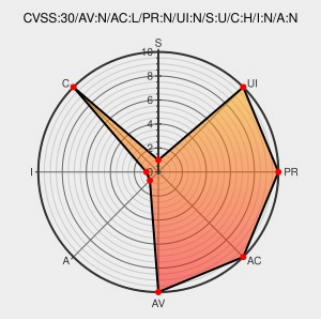
CVE-2017-9132

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

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

CVE-2017-9132

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



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

A hard-coded credentials issue was discovered on Mimosa Client Radios before 2.2.3, Mimosa Backhaul Radios before 2.2.3, and Mimosa Access Points before 2.2.3. These devices run Mosquitto, a lightweight message broker, to send information between devices. By using the vendor's hard-coded credentials to connect to the broker on any device (whether it be an AP, Client, or Backhaul model), an attacker can view all the messages being sent between the devices. If an attacker connects to an AP, the AP will leak information about any clients connected to it, including the serial numbers, which can be used to remotely factory reset the clients via a page in their web interface.

CVE-2017-9132 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: 5 - MEDIUM

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