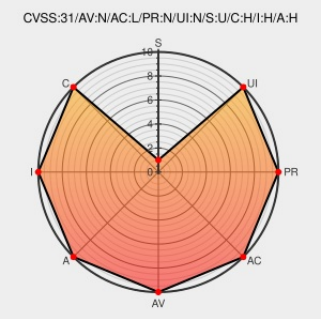
CVE-2018-7081

Published on: 09/13/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:38 PM UTC

CVE-2018-7081

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



Certain versions of Arubaos from Arubanetworks contain the following vulnerability:

A remote code execution vulnerability is present in network-listening components in some versions of ArubaOS. An attacker with the ability to transmit specially-crafted IP traffic to a mobility controller could exploit this vulnerability and cause a process crash or to execute arbitrary code within the underlying operating system with full system privileges. Such an attack could lead to complete system compromise. The ability to transmit traffic to an IP interface on the mobility controller is required to carry out an attack. The attack leverages the PAPI protocol (UDP port 8211). If the mobility controller is only bridging L2 traffic to an uplink and does not have an IP address that is accessible to the attacker, it cannot be attacked.

CVE-2018-7081 has been assigned by security-alert@hpe.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
Remote Code Execution in Aruba Mobility Controller (ArubaOS) - CVE-2018-7081 :: DoomsDay Vault	Exploit Third Party Advisory x-c3ll.github.io text/html	MISC x-c3ll.github.io/posts/CVE-2018-7081-RCE-ArubaOS/
	Vendor Advisory www.arubanetworks.com text/plain	CONFIRM www.arubanetworks.com/assets/alert/ARUBA-PSA-2019-004.txt

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Arubanetworks	Arubaos	All	All	All	All
Operating System	Arubanetworks	Arubaos	All	All	All	All

cpe:2.3:o:arubanetworks:arubaos:*:*:*:*:*:*:*:*:

cpe:2.3:o:arubanetworks:arubaos:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→