



CVE-2023-22757

Published on: Not Yet Published

Last Modified on: 03/10/2023 07:00:00 PM UTC

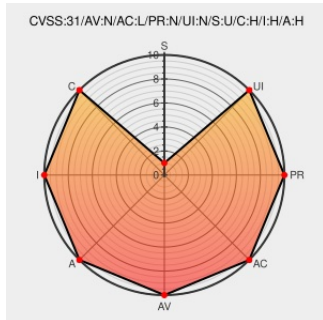
CVE-2023-22757

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Arubaos](#) from [Arubanetworks](#) contain the following vulnerability:

There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying

operating system.

CVE-2023-22757 has been assigned by security-alert@hpe.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Hewlett Packard Enterprise \(HPE\)](#) - **Aruba Mobility Conductor (formerly Mobility Master); Aruba Mobility Controllers; WLAN Gateways and SD-WAN Gateways managed by Aruba Central** version **not down converted**

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

CVE References

Description	Tags	Link
	www.arubanetworks.com text/plain	www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.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.

Related QID Numbers

43989 Hewlett Packard Enterprise (HPE) ArubaOS Unauthenticated Buffer Overflow Vulnerabilities (ARUBA-PSA-2023-002)

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
Operating System	Arubanetworks	Arubaos	All	All	All	All
Application	Arubanetworks	Sd-wan	All	All	All	All
cpe:2.3:o:arubanetworks:arubaos:*.*.*.*.*.*.*.*.						
cpe:2.3:o:arubanetworks:arubaos:*.*.*.*.*.*.*.*.						
cpe:2.3:o:arubanetworks:arubaos:*.*.*.*.*.*.*.*.						
cpe:2.3:a:arubanetworks:sd-wan:*.*.*.*.*.*.*.*.						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-22757 : There are buffer overflow vulnerabilities in multiple underlying operating system processes that c... twitter.com/i/web/status/1...	2023-03-01 08:12:45
 /r/netcve	CVE-2023-22757	2023-03-01 08:38:28
 /r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Aruba Products Could Allow for Arbitrary Code Execution - PATCH NOW - TLP: CLEAR	2023-03-01 15:46:44

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report