

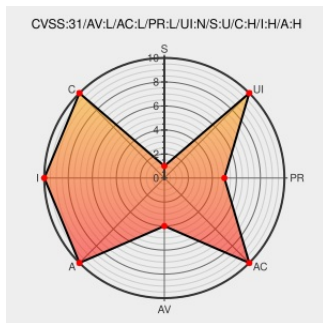


CVE-2023-25590

Published on: Not Yet Published

Last Modified on: 03/27/2023 06:03:00 PM UTC

CVE-2023-25590

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Clearpass Policy Manager](#) from [Arubanetworks](#) contain the following vulnerability:

A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance.

CVE-2023-25590 has been assigned by [security-alert@hpe.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Hewlett Packard Enterprise \(HPE\)](#) - [Aruba ClearPass Policy Manager](#) version = **6.11.1 and below**

Affected Vendor/Software: [Hewlett Packard Enterprise \(HPE\)](#) - [Aruba ClearPass Policy Manager](#) version = **6.10.8 and below**

Affected Vendor/Software: [Hewlett Packard Enterprise \(HPE\)](#) - [Aruba ClearPass Policy Manager](#) version = **6.9.13 and below**

CVSS3 Score: **7.8 - HIGH**

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

CVE References

Description	Tags	Link
	www.arubanetworks.com text/plain	MISC www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.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
Application	Arubanetworks	Clearpass Policy Manager	6.11.0	All	All	All
Application	Arubanetworks	Clearpass Policy Manager	6.11.1	All	All	All
Application	Arubanetworks	Clearpass Policy Manager	All	All	All	All
Application	Arubanetworks	Clearpass Policy Manager	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All

```
cpe:2.3:a:arubanetworks:clearpass_policy_manager:6.11.0:*:*:*:*:*:
```

```
cpe:2.3:a:arubanetworks:clearpass_policy_manager:6.11.1:*.*.*.*.*.:
```

```
cpe:2.3:a:arubanetworks:clearpass_policy_manager:*.*.*.*.*.*:
```

```
cpe:2.3:a:arubanetworks:clearpass_policy_manager:*.*.*.*.*.*.*:
```

```
cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-25590 : A vulnerability in the ClearPass OnGuard #Linux agent could allow malicious users on a Linux insta... twitter.com/i/web/status/1...	2023-03-22 06:05:39
 /r/netcve	CVE-2023-25590	2023-03-22 07:38:39

[← 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