



# CVE-2017-5825

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2017-5825
<b>State</b>	PUBLIC
<b>Assigner</b>	security-alert@hpe.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-02-15 22:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	A privilege escalation vulnerability in HPE Aruba ClearPass Policy Manager version 6.6.x was found.

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Hp</a>	<a href="#">Aruba Clearpass Policy Manager</a>	All	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Aruba Clearpass Policy Manager</a>	All	All	All	All

## References

Reference	Source	Link	Tags
ClearPass Policy Manager Multiple Security Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory, VDB Entry
<a href="http://www.arubanetworks.com/assets/alert/HPESBHF03730.txt">www.arubanetworks.com/assets/alert/HPESBHF03730.txt</a>	CONFIRM	<a href="http://www.arubanetworks.com">www.arubanetworks.com</a>	Third Party Advisory
HPE Support document - HPE Support Center	CONFIRM	<a href="http://support.hpe.com">support.hpe.com</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)**