CVE-2020-7110

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-7110
State	PUBLIC
Assigner	security-alert@hpe.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-16 19:15:00 UTC
Updated	2020-04-22 17:50:00 UTC
Description	ClearPass is vulnerable to Stored Cross Site Scripting by allowing a malicious administrator, or a compromised administrat

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arubanetworks	Clearpass	All	All	All	All
Application	Arubanetworks	Clearpass	All	All	All	All

References

Reference	Source	Link	Tags
www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-004.txt	MISC	www.arubanetworks.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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