CVE-2018-7636

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

Summary

CVE	CVE-2018-7636
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-03 21:29:00 UTC
Updated	2020-02-17 16:15:00 UTC
Description	The URL filtering "continue page" hosted by PAN-OS 8.0.10 and earlier may allow an attacker to inject arbitrary JavaScript

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Paloaltonetworks	Pan-os	8.0.10	All	All	All
Operating System	Paloaltonetworks	Pan-os	8.0.10	All	All	All

References

Reference
CVE-2018-7636 Cross Site Scripting in PAN-OS
Palo Alto Networks PAN-OS CVE-2018-7636 Cross Site Scripting Vulnerability
Palo Alto PAN-OS Input Validation Flaw in URL Filtering 'continue page' Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTr
CVE Program record
NVD vulnerability detail

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