



CVE-2018-10140

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-10140
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-16 18:29:00 UTC
Updated	2020-02-17 16:15:00 UTC
Description	The PAN-OS Management Web Interface in Palo Alto Networks PAN-OS 8.1.2 and earlier may allow an authenticated user

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Palo Alto PAN-OS Management Web Interface Bug Lets Remote Authenticated Users Deny Service - SecurityTracker	SECTRACK	www.s...
Palo Alto Networks PAN-OS CVE-2018-10140 Denial of Service Vulnerability	BID	www.s...
CVE-2018-10140 Denial of Service in PAN-OS Management Web Interface	CONFIRM	securi...
CVE Program record	CVE.ORG	www.c...
NVD vulnerability detail	NVD	nvd.ni...

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](#).

Free CVE JSON API cve.report/api

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