CVE-2021-3056

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

Summary

CVE	CVE-2021-3056
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-10 17:15:00 UTC
Updated	2021-11-15 13:03:00 UTC
Description	A memory corruption vulnerability in Palo Alto Networks PAN-OS GlobalProtect Clientless VPN enables an authenticated a

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Paloaltonetworks	Pan-os	All	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.0.0	All	All	All

References

Reference	Source	Link
CVE-2021-3056 PAN-OS: Memory Corruption Vulnerability in GlobalProtect Clientless VPN During SAML Authentication	CONFIRM	secur
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was found by Nicholas Newsom of Palo Alto Networks during an internal security review.

Legacy QID Mappings

730273 Palo Alto Networks (PAN-OS) GlobalProtect Memory Corruption Vulnerability (PAN-149501)

Free CVE JSON API cve.report/api

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