



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	secu
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)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)