CVE-2021-3062

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

Summary

CVE	CVE-2021-3062
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-10 17:15:00 UTC
Updated	2022-07-25 10:53:00 UTC
Description	An improper access control vulnerability in PAN-OS software enables an attacker with authenticated access to GlobalProte

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Paloaltonetworks	Pan-os	All	All	All	All
Application	Paloaltonetworks	Vm-series Firewall	-	All	All	All

References

Reference	Sourc
CVE-2021-3062 PAN-OS: Improper Access Control Vulnerability Exposing AWS Instance Metadata Endpoint to GlobalProtect Users	CONF
CVE Program record	CVE.C
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Palo Alto Networks thanks Matthew Flanagan of Computer Systems Australia (CSA) for discovering and reporting this issue.

Legacy QID Mappings

730275 Palo Alto Networks (PAN-OS) GlobalProtect Improper Access Control Vulnerability (PAN-164422)

Free CVE JSON API cve.report/api

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