CVE-2019-1579

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

Summary

CVE	CVE-2019-1579
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-19 22:15:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	Remote Code Execution in PAN-OS 7.1.18 and earlier, PAN-OS 8.0.11-h1 and earlier, and PAN-OS 8.1.2 and earlier with C

Risk And Classification

EPSS: 0.930080000 probability, percentile 0.997860000 (date 2026-05-08)

CISA KEV: Listed on 2022-01-10; due 2022-07-10; ransomware use Known

Problem Types: CWE-134

CISA Known Exploited Vulnerability

Vendor	Palo Alto Networks
Product	PAN-OS
Name	Palo Alto Networks PAN-OS Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2019-1579

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	All	All	All	All
Operating System	Paloaltonetworks	Pan-os	All	All	All	All

References

Reference	Source	Link
CVE-2019-1579 Remote Code Execution in GlobalProtect Portal/Gateway Interface	MISC	security.paloalto
Attacking SSL VPN - Part 1: PreAuth RCE on Palo Alto GlobalProtect, with Uber as Case Study! | DEVCORE	MISC	devco.re

Security Advisory	CONFIRM	psirt.global.soni
Palo Alto Networks PAN-OS CVE-2019-1579 Multiple Remote Code Execution Vulnerabilities	BID	www.securityfoc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.