

CVE-2019-1579

Palo Alto Networks PAN-OS Remote Code Execution Vulnerability

CISA KEV since Jan 10, 2022

Actively exploited

Ransomware use known

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 GlobalProtect Portal or GlobalProtect Gateway Interface enabled may allow an unauthenticated remote attacker to execute arbitrary code.

EVRS 77/₁₀₀ Urgent priority	CVSS V3.1 8.1 High · NVD	EPSS 0.462 98.8th percentile · FIRST	CISA DEADLINE Jul 10, 2022 KEV since 2022 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.462 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
pan-os	< 7.1.19 ≥ 8.0.0 < 8.0.12 ≥ 8.1.0 < 8.1.3	7.1.19 · 8.0.12 · 8.1.3	NVD

Sources

Vendor guidance github.com/advisories/GHSA-3w36-wf5x-rjfv
NVD nvd.nist.gov/vuln/detail/CVE-2019-1579

Additional guidance security.paloaltonetworks.com/CVE-2019-1579
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2019-10136

Current data evulnable.com/vulnerability-management/cve/CVE-2019-1579

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.