CVE-2022-0028

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

Summary

CVE	CVE-2022-0028
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-10 16:15:00 UTC
Updated	2022-08-24 13:26:00 UTC
Description	A PAN-OS URL filtering policy misconfiguration could allow a network-based attacker to conduct reflected and amplified TC

Risk And Classification

EPSS: 0.046820000 probability, percentile 0.894460000 (date 2026-05-18)

CISA KEV: Listed on 2022-08-22; due 2022-09-12; ransomware use Unknown

Problem Types: NVD-CWE-Other

CISA Known Exploited Vulnerability

Vendor	Palo Alto Networks
Product	PAN-OS
Name	Palo Alto Networks PAN-OS Reflected Amplification Denial-of-Service Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://security.paloaltonetworks.com/CVE-2022-0028; https://nvd.nist.gov/vuln/detail/CVE-2022-0028

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
CVE-2022-0028 PAN-OS: Reflected Amplification Denial-of-Service (DoS) Vulnerability in URL Filtering	CONFIRM	security.paloaltonetwo
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Palo Alto Networks thanks CERT-XLM for reporting this issue.

Legacy QID Mappings

730595 Palo Alto Networks (PAN-OS) Reflected Amplification Denial of Service (DoS) Vulnerability (PAN-192999)