CVE-2020-2021

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

Summary

CVE	CVE-2020-2021
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-29 15:15:00 UTC
Updated	2020-07-06 14:39:00 UTC
Description	When Security Assertion Markup Language (SAML) authentication is enabled and the 'Validate Identity Provider Certificate'

Risk And Classification

EPSS: 0.189580000 probability, percentile 0.953470000 (date 2026-05-06)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Known

Problem Types: CWE-347

CISA Known Exploited Vulnerability

Vendor	Palo Alto Networks
Product	PAN-OS
Name	Palo Alto Networks PAN-OS Authentication Bypass Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-2021

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	Tags
CVE-2020-2021 PAN-OS: Authentication Bypass in SAML Authentication	CONFIRM	security.paloaltonetworks.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical

NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

Vendor Comments And Credit

Discovery Credit

LEGACY: Palo Alto Networks thanks Salman Khan from the Cyber Risk and Resilience Team and Cameron Duck from the Identity Services Team at Monash University for discovering and reporting this issue.

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