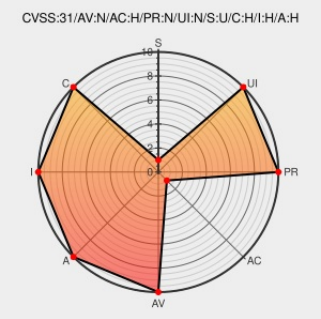
CVE-2020-2001

Published on: 05/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:07 PM UTC

CVE-2020-2001

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pan-os from Paloaltonetworks contain the following vulnerability:

An external control of path and data vulnerability in the Palo Alto Networks PAN-OS Panorama XSLT processing logic that allows an unauthenticated user with network access to PAN-OS management interface to write attacker supplied file on the system and elevate privileges. This issue affects: All PAN-OS 7.1 Panorama and 8.0 Panorama versions; PAN-OS 8.1 versions earlier than 8.1.12 on Panorama; PAN-OS 9.0 versions earlier than 9.0.6 on Panorama.

CVE-2020-2001 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2020-2001 PAN-OS: Panorama External control of file	Vendor Advisory	MISC

CVE-2020-2001 PAN-OS: Panorama External control of file vulnerability leads to privilege escalation	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-2001

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

730271 Palo Alto Networks (PAN-OS) Panorama External control of file Vulnerability (PAN-120397)

Known Affected Configurations (CPE V2.3)

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
Operating System	Paloaltonetworks	Pan-os	All	All	All	All

cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*:

cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*:

cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*:

cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*:

Discovery Credit

This issue was found by Ben Nott of Palo Alto Networks during internal security review.

← Previous ID

Next ID→