

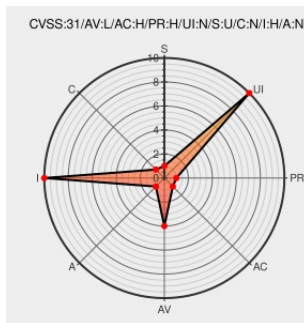


CVE-2020-1994

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

Last Modified on: 03/23/2021 11:23:46 PM UTC

CVE-2020-1994

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Pan-os](#) from [Paloaltonetworks](#) contain the following vulnerability:

A predictable temporary file vulnerability in PAN-OS allows a local authenticated user with shell access to corrupt arbitrary system files affecting the integrity of the system. This issue affects: All versions of PAN-OS 7.1 and 8.0; PAN-OS 8.1 versions earlier than 8.1.13; PAN-OS 9.0 versions earlier than 9.0.7.

CVE-2020-1994 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.4 - MEDIUM**

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

CVSS2 Score: **4.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	COMPLETE	NONE

CVE References

Description	Tags	Link
CVE-2020-1994 PAN-OS: Predictable temporary file vulnerability	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-1994

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.

There are currently no QIDs associated with this CVE

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

Discovery Credit

This issue was found by a customer.

[← Previous ID](#)

[Next ID →](#)