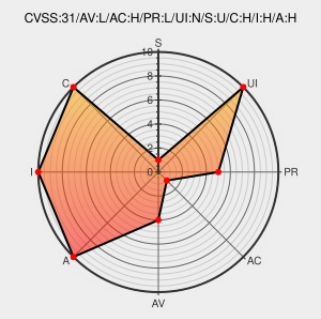
CVE-2020-1981

Published on: 03/11/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:47 PM UTC

CVE-2020-1981

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



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

A predictable temporary filename vulnerability in PAN-OS allows local privilege escalation. This issue allows a local attacker who bypassed the restricted shell to execute commands as a low privileged user and gain root access on the PAN-OS hardware or virtual appliance. This issue affects only PAN-OS 8.1 versions earlier than PAN-OS 8.1.13. This issue does not affect PAN-OS 7.1, PAN-OS 9.0, or later PAN-OS versions.

CVE-2020-1981 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **8.1 < 8.1.13**

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **8.1 !>= 8.1.13**

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **9.0 !>= 9.0.0**

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **7.1 !>= 7.1.0**

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **9.1 !>= 9.1.0**

Vulnerability Patch/Work Around

This issue affects the management interface of PAN-OS and is mitigated by following best practices for securing the PAN-OS management interface. Our best practices guidelines reduce the exposure of the management interface to potential attackers. Please review the Best Practices for Securing Administrative Access in the PAN-OS 8.1 technical documentation, available at: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.

CVSS3 Score: 7.8 - HIGH

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

UNCHANGED | HIGH | HIGH | HIGH

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
CVE-2020-1981 PAN-OS: Predictable temporary filename vulnerability allows local privilege escalation	Issue Tracking Vendor Advisory security.paloaltonetworks.com text/html	CONFIRM security.paloaltonetworks.com/CVE-2020-1981

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

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

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

Discovery Credit

This issue was found during an internal security review.

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report