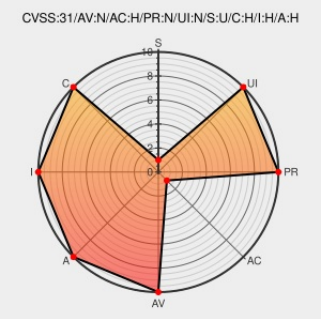
CVE-2020-1979

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

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

CVE-2020-1979

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



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

A format string vulnerability in the PAN-OS log daemon (logd) on Panorama allows a network based attacker with knowledge of registered firewall devices and access to Panorama management interfaces to execute arbitrary code, bypassing the restricted shell and escalating privileges. This issue affects only PAN-OS 8.1 versions earlier than PAN-OS 8.1.13 on Panorama. This issue does not affect PAN-OS 7.1, PAN-OS 9.0, or later PAN-OS versions.

CVE-2020-1979 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 **< 8.1.13**

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

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

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

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

Vulnerability Patch/Work Around

This issue affects the management interface of Panorama and is mitigated by following best practices for securing the Panorama 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**	**Integrity**	**Availability**

	Impact	Impact	Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2020-1979 PAN-OS: A format string vulnerability in PAN-OS log daemon (logd) on Panorama allows local privilege escalation	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-1979

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 discovered by Nicholas Newsom of Palo Alto Networks during an internal security review.

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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