

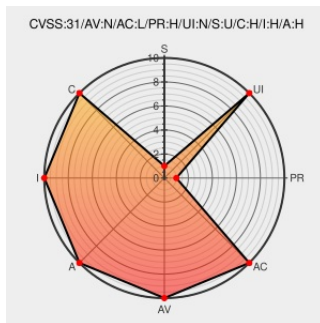


CVE-2020-2027

Published on: 06/10/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:08 PM UTC

CVE-2020-2027

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

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

A buffer overflow vulnerability in the authd component of the PAN-OS management server allows authenticated administrators to disrupt system processes and potentially execute arbitrary code with root privileges. This issue affects: All versions of PAN-OS 7.1 and PAN-OS 8.0; PAN-OS 8.1 versions earlier than PAN-OS 8.1.13; PAN-OS 9.0

versions earlier than PAN-OS 9.0.7.

CVE-2020-2027 has been assigned by [psirt@paloaltonetworks.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Vulnerability Patch/Work Around

This issue affects the management interface of PAN-OS and you can mitigate the impact of this issue by following best practices for securing the PAN-OS management interface. Please review the Best Practices for Securing Administrative Access in the PAN-OS technical documentation, available at <https://docs.paloaltonetworks.com/best-practices>.

CVSS3 Score: **7.2 - HIGH**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
CVE-2020-2027 PAN-OS: Buffer overflow in authd authentication response	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-2027

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

730405 Palo Alto Networks (PAN-OS) Buffer overflow in authd authentication response Vulnerability (CYR-10833)

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:*****:.*						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →