

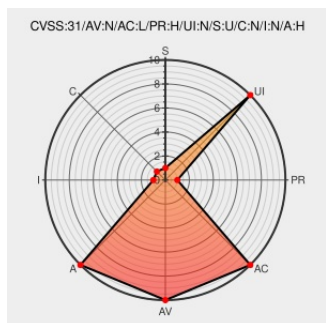


CVE-2020-2031

Published on: 07/08/2020 12:00:00 AM UTC

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

CVE-2020-2031

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

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

An integer underflow vulnerability in the dnspoxyd component of the PAN-OS management interface allows authenticated administrators to issue a command from the command line interface that causes the component to stop responding. Repeated attempts to send this request result in denial of service to all PAN-OS services by restarting the

device and putting it into maintenance mode. This issue impacts: PAN-OS 9.1 versions earlier than PAN-OS 9.1.3. This issue does not impact PAN-OS 8.1, PAN-OS 9.0, or Prisma Access services.

CVE-2020-2031 has been assigned by [psirt@paloaltonetworks.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Palo Alto Networks](#) - **PAN-OS** version < 9.1.3

Affected Vendor/Software: [Palo Alto Networks](#) - **PAN-OS** version !>= 9.1.3

Affected Vendor/Software: [Palo Alto Networks](#) - **PAN-OS** version ! 9.0.*

Affected Vendor/Software: [Palo Alto Networks](#) - **PAN-OS** version ! 8.1.*

Vulnerability Patch/Work Around

This issue impacts the PAN-OS management interface but 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: **4.9 - MEDIUM**

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

UNCHANGED

NONE

NONE

HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
CVE-2020-2031 PAN-OS: Integer underflow in the management interface	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-2031

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

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

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

Discovery Credit

This issue was discovered by Jin Chen of Palo Alto Networks during internal security review.

← Previous ID

Next ID →

