



CVE-2020-2009

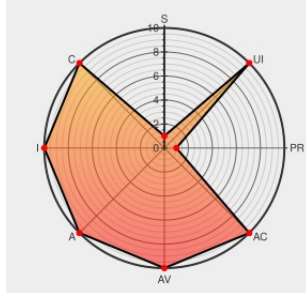
Published on: 05/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:09 PM UTC

CVE-2020-2009

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

CVSS:31/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H



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

An external control of filename vulnerability in the SD WAN component of Palo Alto Networks PAN-OS Panorama allows an authenticated administrator to send a request that results in the creation and write of an arbitrary file on all firewalls managed by the Panorama. In some cases this results in arbitrary code execution with root permissions.

This issue affects: All versions of PAN-OS 7.1; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.7.

CVE-2020-2009 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 is strongly mitigated 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>

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-2020-2009 PAN-OS: Panorama SD WAN arbitrary file creation	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-2009

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

[730270](#) Palo Alto Networks (PAN-OS) Panorama SD WAN arbitrary file creation Vulnerability (PAN-130361)

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:*****:*****:						

Discovery Credit

This issue was found by Nicholas Newsom and Jin Chen of Palo Alto Networks during 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 registered 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](#)