



CVE-2021-3045

Published on: 08/11/2021 12:00:00 AM UTC

Last Modified on: 08/19/2021 06:19:00 PM UTC

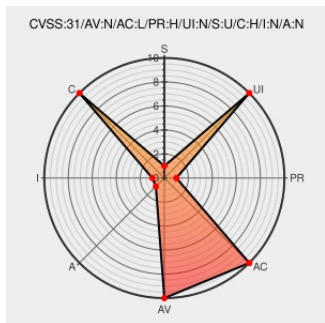
CVE-2021-3045

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

An OS command argument injection vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator to read any arbitrary file from the file system. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.19; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14; PAN-OS 9.1 versions earlier than PAN-OS 9.1.10. PAN-OS 10.0 and later versions are not impacted.

CVE-2021-3045 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as **MEDIUM** severity.

Vulnerability Patch/Work Around

This issue requires the attacker to have authenticated access to the PAN-OS web interface. You can mitigate the impact of this issue by following best practices for securing the PAN-OS web interface. Please review the Best Practices for Securing Administrative Access in the PAN-OS technical documentation 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	HIGH	NONE	NONE

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
CVE-2021-3045 PAN-OS: OS Command Argument Injection in Web Interface	security.paloaltonetworks.com text/html	 MISC security.paloaltonetworks.com/CVE-2021-3045

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

[730158](#) Palo Alto Networks PAN-OS OS Command Argument Injection in Web Interface(PAN-147781)

Exploit/POC from Github

PoC for exploiting CVE-2021-3045 : An OS command argument injection vulnerability in the Palo Alto Networks PAN-OS we...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Paloaltonetworks	Pan-os	All	All	All	All
cpe:2.3:o:paloaltonetworks:pan-os.*.*.*.*.*.*.*.*.*.*						

Discovery Credit

Palo Alto Networks thanks Brandon Vincent for discovering and reporting this issue.

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-3045 : An OS command argument injection vulnerability in the Palo Alto Networks PAN-OS web interface enabl... twitter.com/i/web/status/1...	2021-08-11 17:16:40

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#).

