

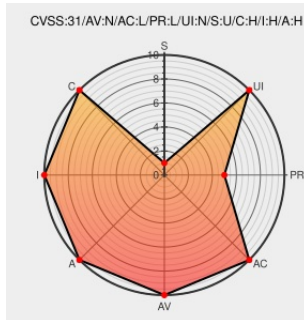


CVE-2021-3050

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

Last Modified on: 08/19/2021 06:49:00 PM UTC

CVE-2021-3050

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

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

An OS command injection vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator to execute arbitrary OS commands to escalate privileges. This issue impacts: PAN-OS 9.0 version 9.0.10 through PAN-OS 9.0.14; PAN-OS 9.1 version 9.1.4 through PAN-OS 9.1.10; PAN-OS 10.0 version 10.0.7

and earlier PAN-OS 10.0 versions; PAN-OS 10.1 version 10.1.0 through PAN-OS 10.1.1. Prisma Access firewalls and firewalls running PAN-OS 8.1 versions are not impacted by this issue.

CVE-2021-3050 has been assigned by [psirt@paloaltonetworks.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Palo Alto Networks is not aware of any malicious exploitation of this issue. However, exploits for this issue are publicly available.

Vulnerability Patch/Work Around

Enable signatures for Unique Threat ID 91439 on traffic destined for the web interface to block attacks against CVE-2021-3050. 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: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	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-2021-3050 PAN-OS: OS Command Injection Vulnerability in Web Interface	security.paloaltonetworks.com text/html	 MISC security.paloaltonetworks.com/CVE-2021-3050

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

730156 Palo Alto Networks PAN-OS OS Command Injection Vulnerability in Web Interface (PAN-174326)

Exploit/POC from Github

PoC for exploiting CVE-2021-3050 : An OS command injection vulnerability in the Palo Alto Networks PAN-OS web interfa...

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

This issue was found by an external security researcher.

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-3050 : An OS command injection vulnerability in the Palo Alto Networks PAN-OS web interface enables an aut... twitter.com/i/web/status/1...	2021-08-11 17:18:13
 /r/cybersecurity	[Unpatched] CVE-2021-3050 PAN-OS: OS Command Injection Vulnerability in Web Interface	2021-08-16 02:23:24

[← 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)