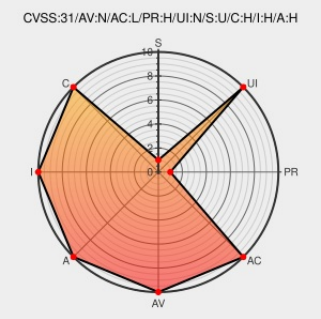
CVE-2020-2037

Published on: 09/09/2020 12:00:00 AM UTC

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

CVE-2020-2037

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 PAN-OS management interface that allows authenticated administrators to execute arbitrary OS commands with root privileges. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.10; PAN-OS 9.1 versions earlier than PAN-OS 9.1.3.

CVE-2020-2037 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 attempts to exploit this vulnerability.

Vulnerability Patch/Work Around

This issue impacts the PAN-OS management web interface but you can mitigate the impact of this issue by following best practices for securing the PAN-OS management web 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-2020-2037 PAN-OS: OS command injection vulnerability in the management web interface	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-2037

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

Palo Alto Networks thanks Mikhail Klyuchnikov of Positive Technologies, and Nicholas Newsom of Palo Alto Networks for discovering and reporting this issue.

Social Mentions

Source	Title	Posted (UTC)
@ipssignatures	It's new to me that WatchGuard has a protection/signature/rule for the vulnerability CVE-2020-2037. … twitter.com/i/web/status/1…	2021-04-27 19:02:02
@ipssignatures	It is the first time for me to know a protection/signature/rule for the vulnerability CVE-2020-2037. #Sfqvcenbl2podk	2021-04-27 19:02:02

← Previous ID Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report