

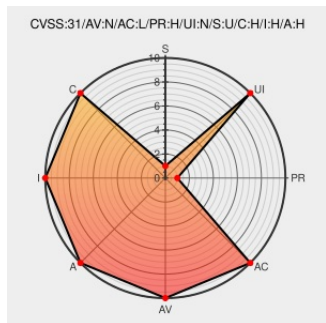


CVE-2020-2038

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

Last Modified on: 10/27/2022 06:18:00 PM UTC

CVE-2020-2038

[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 9.0 versions earlier than 9.0.10; PAN-OS 9.1 versions earlier than 9.1.4; PAN-OS 10.0 versions earlier than 10.0.1.

CVE-2020-2038 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
Palo Alto Networks Authenticated Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/168408/Palo-Alto-Networks-Authenticated-Remote-Code-Execution.html
PAN-OS 10.0 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/168008/PAN-OS-10.0-Remote-Code-Execution.html
CVE-2020-2038 PAN-OS: OS command injection vulnerability in the management web interface	Vendor Advisory security.paloaltonetworks.com text/html	 MISC security.paloaltonetworks.com/CVE-2020-2038

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

Exploit/POC from Github

Exploit to capitalize on vulnerability CVE-2020-2038.

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
<code>cpe:2.3:o:paloaltonetworks:pan-os:*****:.*</code>						
<code>cpe:2.3:o:paloaltonetworks:pan-os:*****:.*</code>						

Discovery Credit

Palo Alto Networks thanks Mikhail Klyuchnikov and Nikita Abramov of Positive Technologies for discovering and reporting this issue.

Social Mentions

Source	Title	Posted (UTC)
 @CisoInvisible	CVE-2020-2038 PAN-OS: OS command injection vulnerability in the management web interface (Severity: HIGH) -... twitter.com/i/web/status/1...	2021-08-13 04:04:28
	It's new to me that CheckPoint has a protection/signature/rule for the vulnerability CVE-2020-2038....	2022-08-21

@ipssignatures	twitter.com/i/web/status/1...	18:02:01
 @ipssignatures	I know one more IPS that has a protection/signature/rule for the vulnerability CVE-2020-2038. ipssignatures.appspot.com/?cve=CVE-2020-... #Spekfrckxmmuh4	2022-08-21 18:02:01
 @ipssignatures	It's new to me that proofpoint has a protection/signature/rule for the vulnerability CVE-2020-2038.... twitter.com/i/web/status/1...	2022-09-01 00:02:00
 @ipssignatures	I know 2 other IPSs that have protections/signatures/rules for the vulnerability CVE-2020-2038. ipssignatures.appspot.com/?cve=CVE-2020-... #Spekfrckxmmuh4	2022-09-01 00:02:01
 @RemotelyAlerts	Severity: ??? An OS Command Injection vulnerability in... CVE-2020-2038 Link for more: alerts.remotelyrmm.com/CVE-2020-2038	2022-09-16 17:29:08
 @ipssignatures	It's new to me that Hillstone has a protection/signature/rule for the vulnerability CVE-2020-2038.... twitter.com/i/web/status/1...	2022-10-15 06:02:01
 @ipssignatures	I know 3 other IPSs that have protections/signatures/rules for the vulnerability CVE-2020-2038. ipssignatures.appspot.com/?cve=CVE-2020-... #Spekfrckxmmuh4	2022-10-15 06:02:01
← 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