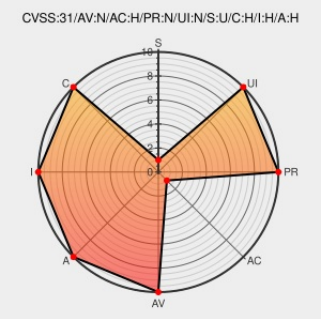
CVE-2020-2034

Published on: 07/08/2020 12:00:00 AM UTC

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

CVE-2020-2034

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 GlobalProtect portal allows an unauthenticated network based attacker to execute arbitrary OS commands with root privileges. An attacker requires some knowledge of the firewall to exploit this issue. This issue can not be exploited if GlobalProtect portal feature is not enabled. This issue impacts PAN-OS 9.1 versions earlier than PAN-OS 9.1.3; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; all versions of PAN-OS 8.0 and PAN-OS 7.1. Prisma Access services are not impacted by this vulnerability.

CVE-2020-2034 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

CVE-2020-2034 PAN-OS: OS command injection vulnerability in GlobalProtect portal	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-2034

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

Determine the Version Running on the Palo Alto Network Firewall for the Global Protect Portal

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 Yamata Li of Palo Alto Networks during internal security review.

Social Mentions

Source	Title	Posted (UTC)
@PrincessYadhavi	Anyone have exploit for paloalto globalprotect portal os command injection? (cve-2020-2034) #bugbountytip… twitter.com/i/web/status/1…	2021-05-06 05:07:11
@PrincessYadhavi	@HackerOn2Wheels Did you get exploit for cve-2020-2034?	2021-05-06 07:58:55
@DFNCERT	PSA: wir haben heute gezielt Einrichtungen mit potenziell verwundbaren Palo Alto PAN-OS (CVE-2020-2034) und Nucleus… twitter.com/i/web/status/1…	2021-11-11 20:26:09
@yYar1ssYy	Looks like CVE-2020-2034 might have been a trivial command injection in the cer parameter of	2021-12-02

@xXcrissXx	Looks like CVE-2020-2034 might have been a trivial command injection in the csr parameter of /global-protect/getsat… twitter.com/i/web/status/1…	2021-12-02 22:54:46
/r/bugbounty	Harder to find POCs	2021-11-20 03:59:19
/r/HowToHack	Harder to find POCs	2021-11-20 15:34:52

← Previous ID

Next ID→