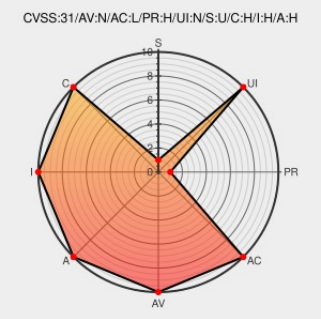
CVE-2020-2006

Published on: 05/13/2020 12:00:00 AM UTC

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

CVE-2020-2006

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pan-os from Paloaltonetworks contain the following vulnerability:

A stack-based buffer overflow vulnerability in the management server component of PAN-OS that allows an authenticated user to potentially execute arbitrary code with root privileges. This issue affects: All versions of PAN-OS 7.1 and 8.0; PAN-OS 8.1 versions earlier than 8.1.14.

CVE-2020-2006 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **< 8.1.14**

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **!>= 8.1.14**

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **= 7.1.***

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **= 8.0.***

Vulnerability Patch/Work Around

This issue affects the management interface of PAN-OS and is strongly mitigated by following best practices for securing the PAN-OS management interface. Please review the Best Practices for Securing Administrative Access in the PAN-OS technical documentation, available at: https://docs.paloaltonetworks.com.

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	Access	Authentication

Vector	Complexity	
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
CVE-2020-2006 PAN-OS: Buffer overflow in management server payload parser	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-2006

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
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:*:*:*:*:*:*:*:*:

Discovery Credit

Palo Alto Networks thanks Jin Chen of Palo Alto Networks for discovering and reporting this issue.

← Previous ID

Next ID→

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