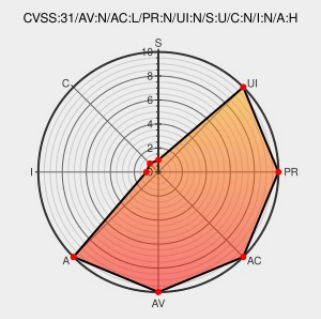
CVE-2020-2011

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

Last Modified on: 03/23/2021 11:24:07 PM UTC

CVE-2020-2011

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



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

An improper input validation vulnerability in the configuration daemon of Palo Alto Networks PAN-OS Panorama allows for a remote unauthenticated user to send a specifically crafted registration request to the device that causes the configuration service to crash. Repeated attempts to send this request result in denial of service to all PAN-OS Panorama services by restarting the device and putting it into maintenance mode. This issue affects: All versions of PAN-OS 7.1, PAN-OS 8.0; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.7; PAN-OS 9.1 versions earlier than 9.1.0.

CVE-2020-2011 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

Vulnerability Patch/Work Around

This issues 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: 7.5 - HIGH

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

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
CVE-2020-2011 PAN-OS: Panorama registration denial of service	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-2011

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
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 Ben Nott of Palo Alto Networks during internal security review.

← 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