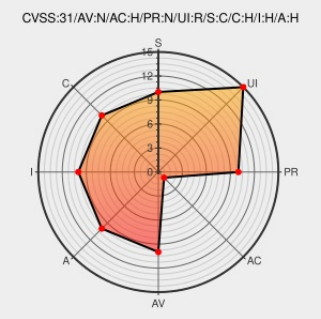
CVE-2020-2013

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

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

CVE-2020-2013

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



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

A cleartext transmission of sensitive information vulnerability in Palo Alto Networks PAN-OS Panorama that discloses an authenticated PAN-OS administrator's PAN-OS session cookie. When an administrator issues a context switch request into a managed firewall with an affected PAN-OS Panorama version, their PAN-OS session cookie is transmitted over cleartext to the firewall. An attacker with the ability to intercept this network traffic between the firewall and Panorama can access the administrator's account and further manipulate devices managed by Panorama. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.13; PAN-OS 9.0 versions earlier than 9.0.6; PAN-OS 9.1 versions earlier than 9.1.1; All version of PAN-OS 8.0;

CVE-2020-2013 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

Vulnerability Patch/Work Around

One possible vulnerability mitigation is to shorten the length of administrator session idle timeout. This reduces the likelihood the exposed administrator's session cookie is valid at time of attack.

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	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2020-2013 PAN-OS: Panorama context switch session cookie disclosure	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-2013

Related QID Numbers

730268 Palo Alto Networks (PAN-OS) Panorama context switch session cookie disclosure (PAN-125122)

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→

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