



CVE-2020-2018

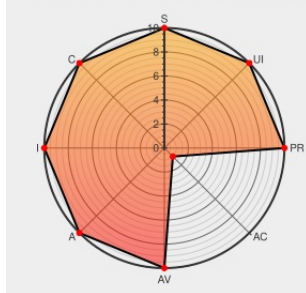
Published on: 05/13/2020 12:00:00 AM UTC

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

CVE-2020-2018

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H



Certain versions of [Pan-os](#) from [Paloaltonetworks](#) contain the following vulnerability:

An authentication bypass vulnerability in the Panorama context switching feature allows an attacker with network access to a Panorama's management interface to gain privileged access to managed firewalls. An attacker requires some knowledge of managed firewalls to exploit this issue. This issue does not affect Panorama

configured with custom certificates authentication for communication between Panorama and managed devices. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.12; PAN-OS 9.0 versions earlier than 9.0.6; All versions of PAN-OS 8.0.

CVE-2020-2018 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as **CRITICAL** severity.

Vulnerability Patch/Work Around

This issue can be completely mitigated by enabling custom certificates authentication between Panorama and managed firewalls. See <https://docs.paloaltonetworks.com/panorama/8-0/panorama-admin/set-up-panorama/set-up-authentication-using-custom-certificates.html> 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: **9 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	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-2020-2018 PAN-OS: Panorama authentication bypass vulnerability	Vendor Advisory security.paloaltonetworks.com text/html	 MISC security.paloaltonetworks.com/CVE-2020-2018

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

This issue was found by Ben Nott of Palo Alto Networks during internal security review.

[← Previous ID](#)

[Next ID →](#)

