



CVE-2020-2017

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

Last Modified on: 03/23/2021 11:24:09 PM UTC

CVE-2020-2017

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

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

A DOM-Based Cross Site Scripting Vulnerability exists in PAN-OS and Panorama Management Web Interfaces. A remote attacker able to convince an authenticated administrator to click on a crafted link to PAN-OS and Panorama Web Interfaces could execute arbitrary JavaScript code in the administrator's browser and perform

administrative actions. 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; All versions of PAN-OS 8.0.

CVE-2020-2017 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as **MEDIUM** severity.

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: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality	Integrity	Availability

Impact

NONE

Impact

PARTIAL

Impact

NONE

CVE References

Description

Tags

Link

CVE-2020-2017 PAN-OS: DOM-Based cross site scripting vulnerability in management web interface

Vendor Advisory

security.paloaltonetworks.com

text/html

MISC

security.paloaltonetworks.com/CVE-2020-2017

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 Chris Ganas of Palo Alto Networks during internal security review.

← Previous ID

Next ID →