

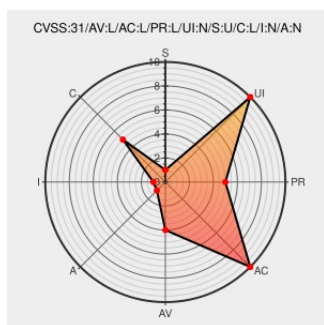


CVE-2020-2043

Published on: 09/09/2020 12:00:00 AM UTC

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

CVE-2020-2043

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

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

An information exposure through log file vulnerability where sensitive fields are recorded in the configuration log without masking on Palo Alto Networks PAN-OS software when the after-change-detail custom syslog field is enabled for configuration logs and the sensitive field appears multiple times in one log entry. The first instance of the

sensitive field is masked but subsequent instances are left in clear text. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.10; PAN-OS 9.1 versions earlier than PAN-OS 9.1.4.

CVE-2020-2043 has been assigned by [psirt@paloaltonetworks.com](#) to track the vulnerability - currently rated as **LOW** severity.

Vulnerability Patch/Work Around

This issue requires access to PAN-OS log files generated in the system. You can mitigate the impact of this issue 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/best-practices>.

CVSS3 Score: **3.3 - LOW**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality	Integrity	Availability

Impact

Impact

Impact

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

CVE-2020-2043 PAN-OS: Passwords may be logged in clear text when using after-change-detail custom syslog field for config logs

Vendor Advisory

security.paloaltonetworks.com

text/html

MISC

security.paloaltonetworks.com/CVE-2020-2043

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 a customer of Palo Alto Networks during internal security review.

← Previous ID

Next ID →