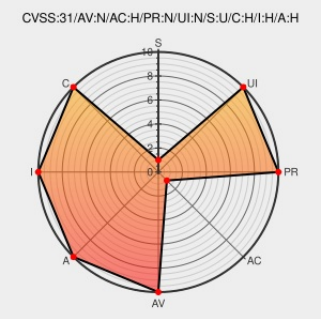
CVE-2020-1992

Published on: 04/08/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:45 PM UTC

CVE-2020-1992

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



Certain versions of Pa-7050 from Paloaltonetworks contain the following vulnerability:

A format string vulnerability in the Varrcvr daemon of PAN-OS on PA-7000 Series devices with a Log Forwarding Card (LFC) allows remote attackers to crash the daemon creating a denial of service condition or potentially execute code with root privileges. This issue affects Palo Alto Networks PAN-OS 9.0 versions before 9.0.7; PAN-OS 9.1 versions before 9.1.2 on PA-7000 Series devices with an LFC installed and configured. This issue requires WildFire services to be configured and enabled. This issue does not affect PAN-OS 8.1 and earlier releases. This issue does not affect any other PA Series firewalls.

CVE-2020-1992 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as CRITICAL severity.

Vulnerability Patch/Work Around

There are no viable workarounds for this issue.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	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-2020-1992 PAN-OS on PA-7000 Series: Varrcvr daemon network-based denial of service or privilege escalation	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-1992

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
Hardware	Paloaltonetworks	Pa-7050	-	All	All	All
Hardware	Paloaltonetworks	Pa-7050	-	All	All	All
Hardware	Paloaltonetworks	Pa-7080	-	All	All	All
Hardware	Paloaltonetworks	Pa-7080	-	All	All	All
Operating System	Paloaltonetworks	Pan-os	All	All	All	All
Operating System	Paloaltonetworks	Pan-os	All	All	All	All

cpe:2.3:h:paloaltonetworks:pa-7050:-:*:*:*:*:*:*:*:

cpe:2.3:h:paloaltonetworks:pa-7050:-:*:*:*:*:*:*:*:

cpe:2.3:h:paloaltonetworks:pa-7080:-:*:*:*:*:*:*:*:

cpe:2.3:h:paloaltonetworks:pa-7080:-:*:*:*:*:*:*:*:

cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*:

cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*:

Discovery Credit

This issue was found by a customer.

← Previous ID

Next ID→

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