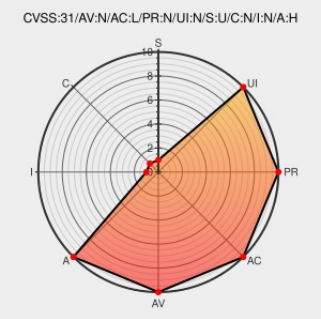
CVE-2021-3053

Published on: 09/08/2021 12:00:00 AM UTC

Last Modified on: 09/15/2021 07:29:00 PM UTC

CVE-2021-3053

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



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

An improper handling of exceptional conditions vulnerability exists in the Palo Alto Networks PAN-OS dataplane that enables an unauthenticated network-based attacker to send specifically crafted traffic through the firewall that causes the service to crash. Repeated attempts to send this request result in denial of service to all PAN-OS services by restarting the device and putting it into maintenance mode. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.20; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14; PAN-OS 9.1 versions earlier than PAN-OS 9.1.9; PAN-OS 10.0 versions earlier than PAN-OS 10.0.5. This issue does not affect Prisma Access.

CVE-2021-3053 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

Palo Alto Networks is not aware of any malicious exploitation of this issue.

Vulnerability Patch/Work Around

There are no known workarounds for this issue.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 7.1 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
CVE-2021-3053 PAN-OS: Exceptional Condition Denial-of-Service (DoS)	security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2021-3053

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.

Related QID Numbers

730192 Palo Alto Networks PAN-OS Exceptional Condition Denial-of-Service Vulnerability (PAN-158723)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Paloaltonetworks	Pan-os	All	All	All	All

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

Discovery Credit

This issue was found by Nicholas Newsom of Palo Alto Networks during internal security review.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3053 : An improper handling of exceptional conditions vulnerability exists in the Palo Alto Networks PAN-O… twitter.com/i/web/status/1…	2021-09-08 17:18:49

← Previous ID

Next ID→