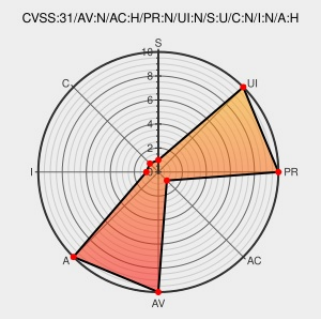
CVE-2021-3048

Published on: 08/11/2021 12:00:00 AM UTC

Last Modified on: 08/19/2021 08:05:00 PM UTC

CVE-2021-3048

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



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

Certain invalid URL entries contained in an External Dynamic List (EDL) cause the Device Server daemon (devsrvr) to stop responding. This condition causes subsequent commits on the firewall to fail and prevents administrators from performing commits and configuration changes even though the firewall remains otherwise functional. If the firewall then restarts, it results in a denial-of-service (DoS) condition and the firewall stops processing traffic. This issue impacts: 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. PAN-OS 8.1 and PAN-OS 10.1 versions are not impacted.

CVE-2021-3048 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as MEDIUM severity.

Vulnerability Patch/Work Around

You can prevent this issue by removing all invalid URL entries from source EDLs or removing the EDL from your configuration. Additionally, do not configure EDLs from websites that you do not trust.

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality	**Integrity**	**Availability**

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
CVE-2021-3048 PAN-OS: Invalid URLs in an External Dynamic List (EDL) can Lead to Firewall Outage	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2021-3048
No Description Provided	security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-3048

Related QID Numbers

730321 Palo Alto Networks (PAN-OS) Invalid URLs in an External Dynamic List (EDL) can Lead to Firewall Outage Vulnerability (PAN-160455)

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 encountered by some customers of Palo Alto Networks during regular operation.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3048 : Certain invalid URL entries contained in an External Dynamic List EDL cause the Device Server dae… twitter.com/i/web/status/1…	2021-08-11 17:17:52

← Previous ID

Next ID→

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