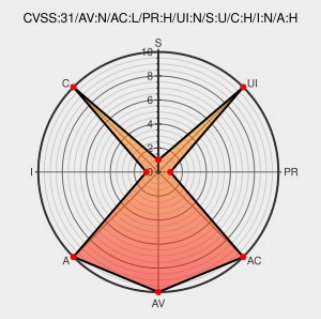
CVE-2021-3055

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

Last Modified on: 09/15/2021 07:04:00 PM UTC

CVE-2021-3055

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



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

An improper restriction of XML external entity (XXE) reference vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator to read any arbitrary file from the file system and send a specifically crafted request to 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 9.1.10; PAN-OS 10.0 versions earlier than PAN-OS 10.0.6. This issue does not affect Prisma Access.

CVE-2021-3055 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as MEDIUM severity.

Palo Alto Networks is not aware of any malicious attempts to exploit this vulnerability.

Vulnerability Patch/Work Around

This issue requires the attacker to have authenticated access to the PAN-OS web interface. You can mitigate the impact of this issue by following best practices for securing the PAN-OS web interface. Please review the Best Practices for Securing Administrative Access in the PAN-OS technical documentation at https://docs.paloaltonetworks.com/best-practices.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	COMPLETE

CVE References

Description	Tags	Link
CVE-2021-3055 PAN-OS: XML External Entity (XXE) Reference Vulnerability in the PAN-OS Web Interface	security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2021-3055

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

730190 Palo Alto Networks PAN-OS XML External Entity (XXE) Reference Vulnerability in the PAN-OS Web Interface (PAN-166241)

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 a customer of Palo Alto Networks during a security review.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3055 : An improper restriction of XML external entity XXE reference vulnerability in the Palo Alto Netwo… twitter.com/i/web/status/1…	2021-09-08 17:19:29

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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