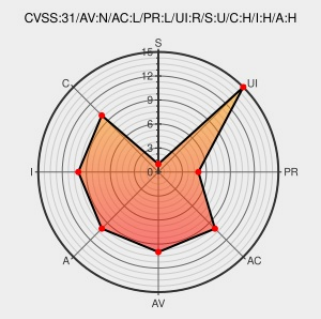
CVE-2021-3052

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

Last Modified on: 09/15/2021 12:18:00 AM UTC

CVE-2021-3052

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



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

A reflected cross-site scripting (XSS) vulnerability in the Palo Alto Network PAN-OS web interface enables an authenticated network-based attacker to mislead another authenticated PAN-OS administrator to click on a specially crafted link that performs arbitrary actions in the PAN-OS web interface as the targeted authenticated administrator. This issue impacts: PAN-OS 8.1 versions earlier than 8.1.20; PAN-OS 9.0 versions earlier than 9.0.14; PAN-OS 9.1 versions earlier than 9.1.10; PAN-OS 10.0 versions earlier than 10.0.2. This issue does not affect Prisma Access.

CVE-2021-3052 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: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
CVE-2021-3052 PAN-OS: Reflected Cross-Site Scripting (XSS) in Web Interface	security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2021-3052

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

730193 Palo Alto Networks PAN-OS Reflected Cross-Site Scripting (XSS) in Web Interface (PAN-150337)

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

Palo Alto Networks thanks Cristian Mocanu and Dan Marin of Deloitte for discovering and reporting this issue.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3052 : A reflected cross-site scripting #XSS vulnerability in the Palo Alto Network PAN-OS web interface… twitter.com/i/web/status/1…	2021-09-08 17:18:36
@Marchal___	CVE-2021-3052 PAN-OS: Reflected Cross-Site Scripting (XSS) in Web Interface security.paloaltonetworks.com/CVE-2021-3052	2021-09-09 18:15:14
@CisoInvisible	CVE-2021-3052 PAN-OS: Reflected Cross-Site Scripting (XSS) in Web Interface (Severity: HIGH) -… twitter.com/i/web/status/1…	2021-09-10 06:07:58

← Previous ID

Next ID→

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