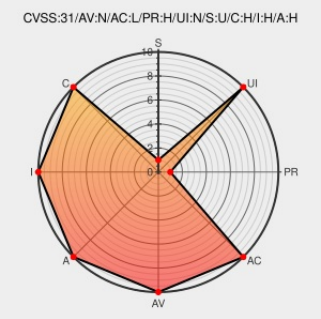
CVE-2021-3054

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

Last Modified on: 09/15/2021 12:20:00 AM UTC

CVE-2021-3054

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



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

A time-of-check to time-of-use (TOCTOU) race condition vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator with permission to upload plugins to execute arbitrary code with root user privileges. 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 9.1.11; PAN-OS 10.0 versions earlier than PAN-OS 10.0.7; PAN-OS 10.1 versions earlier than PAN-OS 10.1.2. This issue does not affect Prisma Access.

CVE-2021-3054 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 exploitation of this issue.

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: 6.6 - MEDIUM

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

CVSS2 Score: 8.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
CVE-2021-3054 PAN-OS: Unsigned Code Execution During Plugin Installation Race Condition Vulnerability	security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2021-3054

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

730191 Palo Alto Networks PAN-OS Unsigned Code Execution During Plugin Installation Race Condition Vulnerability (PAN-138727)

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 Praetorian for discovering and reporting this issue.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3054 : A time-of-check to time-of-use TOCTOU race condition vulnerability in the Palo Alto Networks PAN-… twitter.com/i/web/status/1…	2021-09-08 17:19:15

← Previous ID

Next ID→