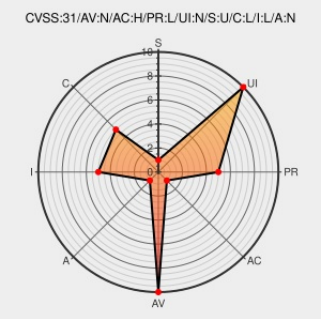
CVE-2021-3047

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

Last Modified on: 08/19/2021 08:03:00 PM UTC

CVE-2021-3047

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



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

A cryptographically weak pseudo-random number generator (PRNG) is used during authentication to the Palo Alto Networks PAN-OS web interface. This enables an authenticated attacker, with the capability to observe their own authentication secrets over a long duration on the PAN-OS appliance, to impersonate another authenticated web interface administrator's session. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.19; 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 10.0.4. PAN-OS 10.1 versions are not impacted.

CVE-2021-3047 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as LOW severity.

Vulnerability Patch/Work Around

There are no known workarounds for this issue.

CVSS3 Score: 3.1 - LOW

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

Impact	Impact	Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
CVE-2021-3047 PAN-OS: Weak Cryptography Used in Web Interface Authentication	security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2021-3047

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

730159 Palo Alto Networks PAN-OS Weak Cryptography Used in Web Interface Authentication(PAN-156240)

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 Google Security for discovering and reporting this issue.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3047 : A cryptographically weak pseudo-random number generator PRNG is used during authentication to the… twitter.com/i/web/status/1…	2021-08-11 17:17:27

← Previous ID

Next ID→

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