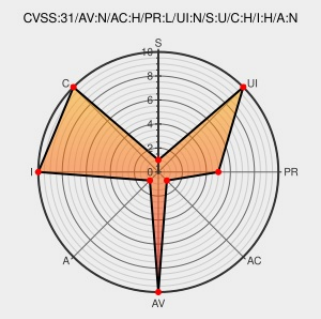
CVE-2021-3046

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

Last Modified on: 08/19/2021 07:08:00 PM UTC

CVE-2021-3046

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



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

An improper authentication vulnerability exists in Palo Alto Networks PAN-OS software that enables a SAML authenticated attacker to impersonate any other user in the GlobalProtect Portal and GlobalProtect Gateway when they are configured to use SAML authentication. 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 9.1.9; PAN-OS 10.0 versions earlier than PAN-OS 10.0.5. PAN-OS 10.1 versions are not impacted.

CVE-2021-3046 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

You can disable SAML authentication for any impacted GlobalProtect portal or gateway until you upgrade the PAN-OS firewall to a fixed version.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
CVE-2021-3046 PAN-OS: Improper SAML Authentication Vulnerability in GlobalProtect Portal	security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2021-3046

Related QID Numbers

730157 Palo Alto Networks PAN-OS Improper SAML Authentication Vulnerability in GlobalProtect Portal (PAN-150023)

Exploit/POC from Github

PoC for exploiting CVE-2021-3046 : An improper authentication vulnerability exists in Palo Alto Networks PAN-OS softw…

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 Alexander Harvey for discovering and reporting this issue.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3046 : An improper authentication vulnerability exists in Palo Alto Networks PAN-OS software that enables… twitter.com/i/web/status/1…	2021-08-11 17:16:59

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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