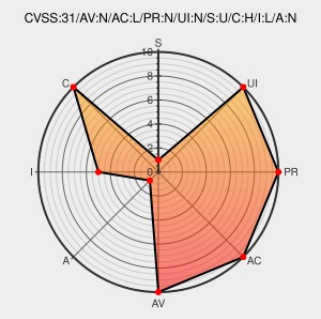
CVE-2020-2050

Published on: 11/11/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:09 PM UTC

CVE-2020-2050

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



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

An authentication bypass vulnerability exists in the GlobalProtect SSL VPN component of Palo Alto Networks PAN-OS software that allows an attacker to bypass all client certificate checks with an invalid certificate. A remote attacker can successfully authenticate as any user and gain access to restricted VPN network resources when the gateway or portal is configured to rely entirely on certificate-based authentication. Impacted features that use SSL VPN with client certificate verification are: GlobalProtect Gateway, GlobalProtect Portal, GlobalProtect Clientless VPN In configurations where client certificate verification is used in conjunction with other authentication methods, the protections added by the certificate check are ignored as a result of this issue. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.17; PAN-OS 9.0 versions earlier than PAN-OS 9.0.11; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5; PAN-OS 10.0 versions earlier than PAN-OS 10.0.1.

CVE-2020-2050 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

Palo Alto Networks is not aware of any malicious exploitation of this issue.

Vulnerability Patch/Work Around

This issue can be mitigated by configuring GlobalProtect SSL VPN to require gateway and portal users to authenticate with their credentials. Other authentication methods are not impacted by this issue.

CVSS3 Score: 8.2 - HIGH

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

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
CVE-2020-2050 PAN-OS: Authentication bypass vulnerability in GlobalProtect SSL VPN client certificate verification	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-2050

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Paloaltonetworks	Pan-os	All	All	All	All
Operating System	Paloaltonetworks	Pan-os	All	All	All	All

cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*:

cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*:

Discovery Credit

This issue was found by Nicholas Newsom of Palo Alto Networks during internal security review.

Social Mentions

Source	Title	Posted (UTC)
@arvesynd	@bad_packets Looking for CVE-2020-2050? security.paloaltonetworks.com/CVE-2020-2050	2021-05-13 20:10:23
@JimSycurity	@sk0yern @_MG_ By 11/11/20 CVE-2020-2050, a GlobalProtect auth bypass vuln in PAN-OS < 8.1.17 was publicly disclose… twitter.com/i/web/status/1…	2021-11-12 17:10:44
@JimSycurity	@dangoodin001 PAN-OS 8.1.17 was released 9/23/20, designated TAC preferred 10/8/20. CVE-2020-2050, auth bypass in G… twitter.com/i/web/status/1…	2021-11-12 18:01:05

← Previous ID

Next ID→