GlobalProtect App: Certificate Validation Bypass Vulnerabilities

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-0249
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 19:16:59 UTC
Updated	2026-05-14 16:21:23 UTC
Description	Multiple improper certificate validation vulnerabilities in the Palo Alto Networks GlobalProtect™ app enables an attacker to i

Risk And Classification

Primary CVSS: v4.0 4.9 MEDIUM from psirt@paloaltonetworks.com

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:N/R:U/V:D/RE:M/U:Amber

EPSS: 0.000040000 probability, percentile 0.001590000 (date 2026-05-14)

Problem Types: CWE-295 | CWE-295 CWE-295 Improper Certificate Validation

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	4.9	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/S
4.0	CNA	CVSS	4.9	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:N/R:U/V:D/RE:M/U:Amber

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Palo Alto Networks	GlobalProtect App	affected 6.3.0 6.3.3-h9 (6.3.3-999) custom	macOS
CNA	Palo Alto Networks	GlobalProtect App	affected 6.2.0 6.2.8-h10 (6.2.8-948) custom	macOS
CNA	Palo Alto Networks	GlobalProtect App	affected 6.1.0 6.1.13 custom	Android, ChromeOS
CNA	Palo Alto Networks	GlobalProtect App	affected 6.0.0 6.0.14 custom	Android, ChromeOS
CNA	Palo Alto Networks	GlobalProtect App	affected 6.0.0 6.0.13 custom	macOS
CNA	Palo Alto Networks	GlobalProtect App	unaffected All custom	Windows, Linux, iOS, Windows UWP

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0249	psirt@paloaltonetworks.com	security.paloaltonetworks.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Palo Alto Networks thanks Kakao Corp. Service Security Team and our internal security research teams for discovering and reporting this issue. (en)

Additional Advisory Data

Source	Time	Event

CNA	2026-05-13T16:00:00.000Z	Initial publication.

Solutions

CNA: Version Minor Version Suggested Solution GlobalProtect App 6.1 on Android 6.1.0 through 6.1.12 Upgrade to 6.1.13 or later. GlobalProtect App 6.0 on Android 6.0.0 through 6.0.13 Upgrade to 6.0.14 or later. GlobalProtect App 6.1 on Chrome OS 6.1.0 through 6.1.12 Upgrade to 6.1.13 or later. GlobalProtect App 6.0 on Chrome OS 6.0.0 through 6.0.13 Upgrade to 6.0.14 or later. GlobalProtect App 6.3 on macOS 6.3.0 through 6.3.3-h8 Upgrade to 6.3.3-h9 (6.3.3-999) or later. GlobalProtect App 6.2 on macOS 6.2.0 through 6.2.8-h9 Upgrade to 6.2.8-h10 (6.2.8-948) or later. GlobalProtect App 6.0 on macOS 6.0.0 through 6.0.12 Upgrade to 6.0.13 or later. GlobalProtect App on Windows No action needed. GlobalProtect App on Linux No action needed. GlobalProtect App on iOS No action needed. GlobalProtect App on UWP No action needed.

Workarounds

CNA: No known workarounds exist for this issue.

Exploits

CNA: Palo Alto Networks is not aware of any malicious exploitation of these issues.

There are currently no legacy QID mappings associated with this CVE.