GlobalProtect App: Buffer Overflow Vulnerability during connection to Portal or Gateway

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

Summary

CVE	CVE-2026-0250
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	A buffer overflow vulnerability exists in the Palo Alto Networks GlobalProtect™ app that enables a man in the middle attack

Risk And Classification

Primary CVSS: v4.0 5.2 MEDIUM from psirt@paloaltonetworks.com

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/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: 0.000060000 probability, percentile 0.003670000 (date 2026-05-14)

Problem Types: CWE-787 | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	5.2	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	5.2	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/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

High

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:H/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	Windows, MacOS
CNA	Palo Alto Networks	GlobalProtect App	affected 6.2.0 6.2.8-h10 (6.2.8-948) custom	Windows, MacOS
CNA	Palo Alto Networks	GlobalProtect App	affected 6.1 6.1.13 custom	Android, Chrome OS
CNA	Palo Alto Networks	GlobalProtect App	affected 6.3.0 6.3.3-h2 (6.3.3-42) custom	Linux
CNA	Palo Alto Networks	GlobalProtect App	affected 6.0.0 6.0.11 custom	Linux
CNA	Palo Alto Networks	GlobalProtect App	affected 6.0 6.0.13 custom	Windows, MacOS
CNA	Palo Alto Networks	GlobalProtect App	affected 6.0 6.0.14 custom	Android, Chrome OS
CNA	Palo Alto Networks	GlobalProtect UWP App	affected 6.3 6.3.3-h10 custom	Windows
CNA	Palo Alto Networks	GlobalProtect App	unaffected All custom	iOS

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0250	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: our internal security research teams (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 6.3 on Windows 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 Windows 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 Windows 6.0.0 through 6.0.12 Upgrade to 6.0.13 or later. GlobalProtect App 6.0 on Linux 6.0.0 through 6.0.10 Upgrade to 6.0.11 or later. GlobalProtect App 6.2/6.3 on Linux 6.2.0 through 6.3.3-h1 Upgrade to 6.3.3-h2 (6.3.3-42) 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 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 ChromeOS 6.1.0 through 6.1.12 Upgrade to 6.1.13 or later. GlobalProtect App 6.0 on ChromeOS 6.0.0 through 6.0.13 Upgrade to 6.0.14 or later. GlobalProtect UWP App 6.1.0 through 6.3.3-h9 Upgrade to 6.3.3-h10 or later. GlobalProtect App on iOS 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 this issue.

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