



GlobalProtect App: Local Privilege Escalation Vulnerabilities

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-0251
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 local privilege escalation vulnerabilities in the Palo Alto Networks GlobalProtect™ app allow a local user to escalate

Risk And Classification

Primary CVSS: v4.0 5.9 MEDIUM from psirt@paloaltonetworks.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/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/MSX/MSI:X/MSA:X/S:X/AU:N/R:U/V:D/RE:M/U:Amber

EPSS: 0.000060000 probability, percentile 0.003590000 (date 2026-05-14)

Problem Types: CWE-426 | CWE-426 CWE-426 Untrusted Search Path

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	5.9	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	5.9	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/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/MSX/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
CNA	Palo Alto Networks	GlobalProtect App	affected 6.2.0 6.2.8-h10 (6.2.8-948) custom	Windows
CNA	Palo Alto Networks	GlobalProtect App	affected 6.0.0 6.0.13 custom	Windows
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 6.0.0 6.0.13 custom	macOS
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	Global Protect App	unaffected All custom	Android, ChromeOS, iOS, UWP

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0251	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 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 6.0 on Windows 6.0.0 through 6.0.12 Upgrade to 6.0.13 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 6.3 on Windows 6.3.0 through 6.3.3-h8 Upgrade to 6.3.3-h9 (6.3.3-999) or later. GlobalProtect App 6.0 on macOS 6.0.0 through 6.0.12 Upgrade to 6.0.13 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 6.3 on macOS 6.3.0 through 6.3.3-h8 Upgrade to 6.3.3-h9 (6.3.3-999) or later. GlobalProtect App 6.0 on Linux 6.0.0 through 6.0.10 Upgrade to 6.0.11 or later GlobalProtect App 6.2 on Linux 6.2.0 through 6.2.9 Upgrade to 6.3.3-h2 (6.3.3-42) or later. GlobalProtect App 6.3 on Linux 6.3.0 through 6.3.3-h1 Upgrade to 6.3.3-h2 (6.3.3-42) or later. GlobalProtect App on Android No action needed. GlobalProtect App on Chrome OS 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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)