INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-13 14:29 UTC

Palo Alto GlobalProtect App Local Privilege Escalation (CVE-2026-0251), Windows, macOS, Linux

CVE VULNERABILITY | MEDIUM | CVSS 5.0

SCC Item ID	SCC-CVE-2026-0169
Type	CVE Vulnerability
CVE ID	CVE-2026-0251
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Palo Alto Networks GlobalProtect App 6.0.x, 6.2.x, 6.3.x on Windows, macOS, and Linux
Published	2026-05-13T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

Palo Alto Networks disclosed a local privilege escalation vulnerability in GlobalProtect App (CVE-2026-0251) affecting Windows, macOS, and Linux across three active version branches (6.0.x, 6.2.x, 6.3.x). An attacker with any low-level access to an endpoint running GlobalProtect can escalate to full system control, SYSTEM on Windows or root on macOS/Linux, without relying on network access. No workaround exists; patching is the only remediation. No active exploitation has been reported as of disclosure.

Technical Analysis

CVE-2026-0251 is a local privilege escalation vulnerability in Palo Alto Networks GlobalProtect App rooted in CWE-426 (Untrusted Search Path). Affected versions: 6.0.x, 6.2.x, and 6.3.x on Windows, macOS, and Linux. A low-privileged local user can exploit the untrusted search path condition to execute arbitrary code in the context of a privileged process, achieving SYSTEM-level access on Windows or root on macOS/Linux. The attack is local-only; no network exposure or authentication bypass is required, physical or authenticated local access to an endpoint running GlobalProtect is sufficient. MITRE ATT&CK techniques: T1068 (Exploitation for Privilege Escalation), T1574/T1574.007 (Hijack Execution Flow / Path Interception by PATH Environment Variable), T1078.003 (Valid Accounts: Local Accounts). Note: Palo Alto PSIRT advisory cites CVSS 8.5 (high severity); NVD preliminary score is 5.0 pending official vendor publication. The vendor score is operative for prioritization. No CISA KEV listing, no EPSS data, and no active exploitation reported at time of disclosure. Remediation:

upgrade to a fixed GlobalProtect App version per the Palo Alto Networks Security Advisory. No workaround is available.

Action Checklist

1. Detection & Inventory: Identify all endpoints running GlobalProtect App 6.0.x, 6.2.x, or 6.3.x on Windows, macOS, and Linux using your endpoint management or asset inventory tooling. Prioritize endpoints where multiple local user accounts exist, remote desktop is enabled, or contractor/third-party accounts are present, as these increase the attack surface for local exploitation.
2. Detection (EDR/Inventory): Query your EDR and endpoint inventory for GlobalProtect App version strings in the affected ranges. On Windows, check installed software via registry (HKLM\SOFTWARE\Palo Alto Networks\GlobalProtect) or WMI. On macOS/Linux, query package managers or application directories. Review privileged process creation events (Windows Event ID 4688 with elevated tokens; Linux audit logs for setuid/setgid execution) for anomalies on hosts running affected versions.
3. Eradication: Apply the fixed GlobalProtect App version per the Palo Alto Networks PSIRT advisory. No configuration-based workaround exists; version upgrade is the only remediation path. Validate the upgrade completed successfully before marking the host as remediated.
4. Recovery: After patching, re-confirm GlobalProtect App version on updated endpoints via your endpoint management tooling. Review privileged process creation logs on previously affected hosts for any anomalous escalation events occurring prior to patch deployment. Monitor for any post-patch recurrence of CWE-426-related behaviors (unexpected PATH-based process spawning).
5. Post-Incident: Review endpoint agent update processes to ensure GlobalProtect App and similar privileged endpoint security clients are included in your patch SLA tracking. Assess whether local privilege escalation from endpoint security agents is covered in your threat model. Consider whether least-privilege controls on endpoints limit post-escalation attacker movement.

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent and initiate full forensic investigation if log review during recovery identifies any pre-patch occurrences of PanGPS.exe or pangpd spawning unexpected privileged child processes, which would indicate active exploitation occurred before the patch window closed — particularly on hosts with contractor accounts, shared local access, or RDP exposure.
Recovery Notes	After patching all endpoints in scope, verify GlobalProtect App version strings via registry or CLI on each host before closing remediation tickets, and retain those version-confirmation records as closure evidence. Monitor Sysmon Event ID 1 and Linux auditd execve logs scoped to GlobalProtect parent processes for a minimum of 30 days post-patch to detect any CWE-426-related PATH-abuse recurrence or re-introduction of vulnerable versions via imaging or rollback. If the environment includes shared-access endpoints or contractor accounts that had local access during the vulnerability window, treat those hosts as potentially compromised and perform a targeted log review before returning them to normal operational status.

Forensic Artifacts	Windows Registry key HKLM\SOFTWARE\Palo Alto Networks\GlobalProtect and HKLM\SYSTEM\CurrentControlSet\Services\PanGPS — captures the installed version string and confirms the service runs as SYSTEM, establishing the escalation target; preserve before and after patching. | Windows Security Event Log Event ID 4688 (Process Creation) filtered on parent process PanGPS.exe with TokenElevationTypeFull (%%1936) — the specific artifact that CWE-426 exploitation of GlobalProtect on Windows would produce when the vulnerable service spawns an attacker-controlled binary from a PATH-searched directory. | Linux auditd log (/var/log/audit/audit.log) — execve syscall records with euid=0 and auid!=0 where the process ancestry traces back to pangpd (the GlobalProtect daemon on Linux), indicating a non-root user achieved root execution via the vulnerable agent. | Filesystem modification timestamps and SHA-256 hashes of GlobalProtect binary directories — on Windows: C:\Program Files\Palo Alto Networks\GlobalProtect\; on macOS: /Applications/GlobalProtect.app/Contents/MacOS/; on Linux: /opt/paloaltonetworks/globalprotect/ — CWE-426 exploitation may leave a malicious binary planted in a writable directory earlier in the PATH that the GP service resolved, detectable via unexpected file creation timestamps or hash mismatches. | macOS Unified Log entries from the com.paloaltonetworks.globalprotect subsystem collected via: log collect --last 30d --output gp_unified.logarchive — captures GlobalProtect process behavior including any unexpected privilege escalation events on macOS endpoints in the affected 6.0.x, 6.2.x, or 6.3.x version range.

Per-Action IR Details

Containment — Identify all endpoints running GlobalProtect App 6.0.x, 6.2.x, or 6.3.x on Windows, macOS, and Linux using your endpoint management or asset inventory tooling. Prioritize endpoints where local access is shared, remote desktop is enabled, or contractor/third-party accounts exist, as these increase exploitation feasibility.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Run the following on Windows endpoints via PowerShell to enumerate vulnerable GP installations: Get-ItemProperty 'HKLM:\SOFTWARE\Palo Alto Networks\GlobalProtect' | Select-Object DisplayVersion. On macOS: defaults read /Library/Preferences/com.paloaltonetworks.globalprotect.settings | grep -i version. On Linux: dpkg -l 'globalprotect*' or rpm -q globalprotect. Compile results into a CSV and sort by RDP-enabled flag from 'quser /server:' output. Two-person teams can script this across a host list using PsExec or Ansible ad-hoc commands.

Evidence: Before scoping, snapshot the GlobalProtect service account context on Windows by capturing HKLM\SYSTEM\CurrentControlSet\Services\PanGPS (the GlobalProtect system service) to confirm it runs as SYSTEM — this establishes the escalation target baseline. On macOS/Linux, record the owner and SUID/SGID bits on GlobalProtect binaries in /Applications/GlobalProtect.app/Contents/MacOS/ or /opt/paloaltonetworks/globalprotect/ before any changes, as exploitation of CWE-426 (uncontrolled search path) may alter PATH-resolution artifacts or drop intermediary binaries in writable directories.

Detection — Query your EDR and endpoint inventory for GlobalProtect App version strings in the affected ranges. On Windows, check installed software via registry (HKLM\SOFTWARE\Palo Alto Networks\GlobalProtect) or WMI. On macOS/Linux, query package managers or application directories. Review privileged process creation events (Windows Event ID 4688 with elevated tokens; Linux audit logs for setuid/setgid execution) for anomalies on hosts running affected versions.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy Sysmon with a config that captures Event ID 1 (Process Create) and Event ID 10 (Process Access) — filter on parent processes matching PanGPS.exe or globalprotect (the GlobalProtect service) spawning unexpected child processes (cmd.exe, bash, sh, python). On Linux, enable auditd rules: auditctl -a always,exit -F arch=b64 -S execve -F euid=0 -F auid!=0 -k priv_esc_gp. On macOS, use the built-in log stream: log stream --predicate 'processImagePath contains "GlobalProtect" AND eventMessage contains "privilege"' --info. For version enumeration without EDR, use osquery: SELECT name, version FROM programs WHERE name LIKE '%GlobalProtect%';

Evidence: Preserve Windows Security Event Log entries for Event ID 4688 (Process Creation) where the Creator Subject Token Elevation Type is TokenElevationTypeFull (%%1936) and the parent process is PanGPS.exe or pangpd. On Linux, collect /var/log/audit/audit.log entries showing execve syscalls with euid=0 where the calling process traces back to the GlobalProtect daemon (pangpd). On macOS, collect Unified Log entries from the com.paloaltonetworks.globalprotect subsystem. Also capture the filesystem modification timestamps on GlobalProtect binary directories before patching, as CWE-426 exploitation may involve a malicious binary planted in a PATH-searched directory that the GP service invoked with elevated privileges.

Eradication — Apply the fixed GlobalProtect App version per the Palo Alto Networks PSIRT advisory (https://security.paloaltonetworks.com/CVE-2026-0251). No configuration-based workaround exists — version upgrade is the only remediation path. Validate the upgrade completed successfully before marking the host as remediated.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Download the fixed GlobalProtect MSI/PKG/RPM directly from the Palo Alto support portal (support.paloaltonetworks.com) — do not use a cached or mirrored copy. Verify the SHA-256 hash of the installer against the Palo Alto PSIRT advisory before deployment. For bulk Windows deployment without SCCM/Intune, use: msiexec /i GlobalProtect64.msi /quiet /l*v C:\GP_upgrade.log then verify post-install with: Get-ItemProperty 'HKLM:\SOFTWARE\Palo Alto Networks\GlobalProtect' | Select-Object DisplayVersion. On Linux: sudo rpm -Uvh globalprotect-.rpm && rpm -q globalprotect. Log all upgrade results per host to a remediation tracking sheet aligned to your CIS 7.2 remediation process.

Evidence: Before upgrading, forensically preserve the original GlobalProtect binary hashes on affected hosts: Get-FileHash 'C:\Program Files\Palo Alto Networks\GlobalProtect\PanGPS.exe' -Algorithm SHA256 on Windows; shasum -a 256 /Applications/GlobalProtect.app/Contents/MacOS/GlobalProtect on macOS; sha256sum /opt/paloaltonetworks/globalprotect/pangpd on Linux. These baseline hashes allow post-incident comparison to detect whether a threat actor replaced the GP binary or planted a trojanized version in a PATH-searched directory as part of CWE-426 exploitation. Also preserve the installer log (C:\GP_upgrade.log) as remediation evidence.

Recovery — After patching, re-confirm GlobalProtect App version on updated endpoints via your endpoint management tooling. Review privileged process creation logs on previously affected hosts for any anomalous escalation events occurring prior to patch deployment. Monitor for any post-patch recurrence of CWE-426-related behaviors (unexpected PATH-based process spawning).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Post-patch, verify GlobalProtect version via the same registry/CLI queries used in detection. Use a YARA rule targeting the vulnerable version string pattern (GlobalProtect 6\.0\.|6\.2\.|6\.3\.) against the installed binary

to confirm no rollback or re-installation of vulnerable versions. For ongoing PATH-abuse monitoring, deploy a Sigma rule detecting processes spawned by PanGPS.exe or pangpd that are not in the expected GlobalProtect installation directory — the Sigma rule community (github.com/SigmaHQ/sigma) has templates for untrusted parent-child process chains that can be adapted. Review 30 days of prior Sysmon/auditd logs on the highest-risk hosts (shared-access, RDP-enabled) for any historical CWE-426 indicators before closing the incident.

Evidence: Collect a post-patch version confirmation screenshot or exported registry value as remediation closure evidence per NIST IR-5 (Incident Monitoring). Review Windows Security Event Log Event ID 4688 records and Linux audit.log execve entries from the 30 days prior to patch deployment, scoped to parent process PanGPS.exe or pangpd, looking for any child processes that should not exist in normal GlobalProtect operation — these would indicate exploitation occurred before the patch window. Preserve these log exports for the post-incident review.

Post-Incident — Review endpoint agent update processes to ensure GlobalProtect App and similar privileged endpoint security clients are included in your patch SLA tracking. Assess whether local privilege escalation from endpoint security agents is covered in your threat model. Consider whether least-privilege controls on endpoints limit post-escalation attacker movement.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SI-2 (Flaw Remediation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Add GlobalProtect App, along with any other Palo Alto Networks endpoint agents (Cortex XDR, GlobalProtect Gateway), to your formal patch SLA register with a critical/high/medium tiering — this CVE at CVSS 5.0 maps to a standard SLA but the SYSTEM/root escalation impact warrants review of whether your SLA correctly accounts for LPE impact beyond raw CVSS score. For least-privilege hardening without enterprise tooling, use AppLocker (Windows) to restrict process execution in directories outside Program Files, and use sudoers restrictions on Linux to prevent non-admin users from executing binaries in world-writable PATH directories. Document findings in a lessons-learned memo per NIST 800-61r3 §4 and update your threat model to explicitly include privileged endpoint security agents as LPE attack surfaces.

Evidence: Compile the final remediation record including: patch deployment timestamps per host, pre- and post-patch GlobalProtect version strings, any privileged process creation anomalies found during log review, and the list of highest-risk hosts (shared-access, contractor accounts, RDP-enabled) that were prioritized. This record supports the NIST IR-5 (Incident Monitoring) documentation requirement and provides the evidence base for the lessons-learned review. If any pre-patch anomalous escalation events were found in log review, escalate to a full forensic investigation before closing the incident.

Detection Guidance

Primary detection signal: presence of GlobalProtect App 6.0.x, 6.2.x, or 6.3.x in your endpoint inventory constitutes exposure. Query endpoint management platforms (Intune, JAMF, SCCM, or equivalent) for installed application version strings matching those ranges. On Windows: query WMI class Win32_Product or registry path HKLM\SOFTWARE\Palo Alto Networks\GlobalProtect for version. On macOS: check /Applications/GlobalProtect.app/Contents/Info.plist for CFBundleShortVersionString. On Linux: check the installed package version via rpm -q GlobalProtect or dpkg -l | grep GlobalProtect depending on distribution. Behavioral indicators to monitor on affected hosts: Windows Event ID 4688 (process creation) with unexpected parent-child relationships involving PanGPS.exe or PanMSService.exe; creation of new high-privileged processes from non-system parent contexts; Linux auditd records showing privilege transitions (execve syscall, setuid calls) originating from GlobalProtect agent processes. No known public IOCs (hashes, IPs, domains) are associated with active exploitation at time of disclosure.

Framework Mappings

MITRE-ATTACK

- **T1068** — Exploitation for Privilege Escalation
- **T1078.003** — Local Accounts
- **T1574** — Hijack Execution Flow
- **T1574.007** — Path Interception by PATH Environment Variable

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **IR-5** — Incident Monitoring

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1078.003	Local Accounts	Defense-Evasion
T1574	Hijack Execution Flow	Persistence
T1574.007	Path Interception by PATH Environment Variable	Persistence

Sources

Source	URL	Tier
Palo Alto Networks Security Advisories	https://security.paloaltonetworks.com/CVE-2026-0251	T3
CVE-2026-5251 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-5251	T1
How Cloudflare responded to the “Copy Fail” Linux vulnerability	https://blog.cloudflare.com/copy-fail-linux-vulnerability-mitigation/	T3
The Copy Fail: Linux Kernel Local Privilege Escalation - ExtraHop	https://www.extrahop.com/blog/linux-kernel-local-privilege-escalation	T3
CVE-2026-26251 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-26251	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-0251	T1

Generated 2026-05-13 14:29 UTC by TJS Security Command Center