INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-14 06:53 UTC

CVE-2026-0250: Palo Alto GlobalProtect Buffer Overflow Enables SYSTEM-Level Code Execution via MitM

CVE VULNERABILITY | MEDIUM | CVSS 5.0

SCC Item ID	SCC-CVE-2026-0177
Type	CVE Vulnerability
CVE ID	CVE-2026-0250
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Palo Alto Networks GlobalProtect App (Windows, macOS, Linux, Android, ChromeOS) versions 6.0.x, 6.1.x, 6.2.x, 6.3.x; GlobalProtect UWP App 6.3.x on Windows. iOS not affected.
Published	2026-05-13T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

A buffer overflow vulnerability in Palo Alto Networks GlobalProtect VPN clients allows an attacker positioned on the same network segment to corrupt memory and execute code with full SYSTEM privileges on affected endpoints. All major platforms are affected across versions 6.0 through 6.3, including Windows, macOS, Linux, Android, and ChromeOS. Patches were released May 13, 2026; the formal CVSS score may understate operational risk because successful exploitation grants the highest privilege level on enterprise VPN clients, which are often trusted and widely deployed.

Technical Analysis

CVE-2026-0250 is a memory corruption vulnerability (CWE-787: Out-of-Bounds Write; CWE-119: Improper Restriction of Memory Buffer Operations) in the Palo Alto Networks GlobalProtect App. An attacker with a man-in-the-middle (MitM) position on the adjacent network can corrupt heap or stack memory during Portal/Gateway TLS communication, potentially achieving arbitrary code execution at SYSTEM privilege level. Affected versions: GlobalProtect App 6.0.x, 6.1.x, 6.2.x, 6.3.x on Windows, macOS, Linux, Android, and ChromeOS; GlobalProtect UWP App 6.3.x on Windows. iOS is confirmed unaffected. MITRE technique coverage includes T1190 (Exploit Public-Facing Application), T1068 (Exploitation for Privilege Escalation), T1203 (Exploitation for Client Execution), and T1557 (Adversary-in-the-Middle). CVSS base score is 5.0

(Medium); EPSS score not yet available and the vulnerability is not on CISA KEV as of this writing. No active exploitation has been observed. Palo Alto Networks confirmed internal discovery. Patches published across all affected branches on May 13, 2026. Source: Palo Alto Networks Security Advisory (official vendor advisory; human validation of specific build numbers recommended); NVD record at https://nvd.nist.gov/vuln/detail/CVE-2026-0250.

Action Checklist

1. Discovery/Identification: Identify all endpoints running GlobalProtect App 6.0.x, 6.1.x, 6.2.x, or 6.3.x on Windows, macOS, Linux, Android, or ChromeOS, and GlobalProtect UWP App 6.3.x on Windows. Prioritize endpoints that connect from untrusted or public networks (hotels, conferences, shared Wi-Fi) where network adjacency assumptions cannot be enforced. Restrict gateway access for unpatched clients if your GlobalProtect configuration supports enforcing minimum client versions. Source: Palo Alto Networks Security Advisory CVE-2026-0250.
2. Detection: Query your endpoint management or MDM inventory for GlobalProtect App version strings matching 6.0.x, 6.1.x, 6.2.x, or 6.3.x (pre-patch). In SIEM, review GlobalProtect gateway logs for anomalous TLS negotiation failures or repeated connection resets from the same source, which may indicate MitM probe activity. No public IOCs are currently available; exploitation attempts would appear at the network layer before client-side logging triggers.
3. Eradication: Apply the patches published by Palo Alto Networks on May 13, 2026, for all affected branches (6.0.x, 6.1.x, 6.2.x, 6.3.x). Obtain the updated installers directly from the Palo Alto Networks support portal at https://support.paloaltonetworks.com (official vendor portal; human validation recommended for specific build numbers). For Android and ChromeOS deployments, push updates via your MDM. Confirm iOS clients are unaffected and do not require action.
4. Recovery: After patching, verify client version strings via endpoint management tooling to confirm all devices are running patched builds. Re-run your GlobalProtect gateway connection health checks to confirm normal TLS handshake behavior. Monitor gateway and endpoint logs for 48 to 72 hours post-patch for any anomalous connection patterns that may indicate prior exploitation attempts that went undetected.
5. Post-Incident: Review whether your network segmentation and VPN architecture relies on adjacency assumptions that a MitM attacker could challenge (e.g., split-tunnel configurations, public Wi-Fi usage policies). Evaluate whether your GlobalProtect deployment enforces minimum client version at the gateway level; if not, this is a control gap to remediate. Document any endpoints that were slow to patch and apply a risk-based review of activity logs for those devices covering the exposure window.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate to senior IR leadership and initiate breach notification assessment if forensic review of any endpoint that connected from an untrusted network during the exposure window (pre-May 13, 2026 patch) reveals SYSTEM-level process creation anomalies (Event ID 4688 with PanGPS.exe or PanGPA.exe as parent), unauthorized scheduled tasks or LaunchDaemon entries, or new registry Run key entries — any of which would indicate successful exploitation of CVE-2026-0250 and potential post-exploitation persistence requiring regulatory breach notification evaluation under applicable frameworks (e.g., GDPR 72-hour notification, HIPAA Breach Notification Rule, or SEC Material Cybersecurity Incident disclosure).
Recovery Notes	After confirming all GlobalProtect clients are running post-May 13, 2026 patched builds across all affected branches (6.0.x, 6.1.x, 6.2.x, 6.3.x), conduct a targeted 72-hour gateway monitoring period focused specifically on TLS handshake anomalies and any SYSTEM-context process lineage from PanGPS.exe or PanGPA.exe on previously high-risk endpoints. For endpoints confirmed to have connected exclusively from corporate network segments with enforced adjacency controls during the entire exposure window, recovery risk is low and standard patch verification suffices; endpoints with documented public Wi-Fi sessions during the exposure window warrant full forensic triage before being returned to unrestricted operation. Enforce GlobalProtect minimum client version at the gateway level as a permanent control to prevent future deployment drift from creating a similar exposure window.
Forensic Artifacts	GlobalProtect client diagnostic logs on Windows (C:\Program Files\Palo Alto Networks\GlobalProtect\PanGPA.log and PanGPS.log) and macOS (/Library/Logs/PaloAlto/GlobalProtect/PanGPA.log) — these record TLS negotiation details, connection state transitions, and error codes that would reflect MitM-induced handshake manipulation targeting the buffer overflow trigger in CVE-2026-0250. | Windows Security Event Log Event ID 4688 (Process Creation) filtered for PanGPS.exe or PanGPA.exe as ParentProcessName with ChildProcessName of cmd.exe, powershell.exe, wscript.exe, or mshta.exe — successful SYSTEM-level code execution from CVE-2026-0250 exploitation would manifest as an unexpected child shell spawned from the GlobalProtect service process. | PAN-OS GlobalProtect gateway System and Traffic logs filtered for the exposure window (pre-May 13, 2026), specifically SSL/TLS handshake failure events, repeated authentication attempts, and tunnel negotiation resets from source IPs geolocated to public Wi-Fi ranges — these represent the network-layer footprint of MitM probe or exploitation activity before client-side logging triggers. | Windows Scheduled Tasks (via 'Get-ScheduledTask' or schtasks /query /fo LIST /v) and Registry Run keys (HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon) with creation or modification timestamps during the exposure window — SYSTEM-level persistence is the expected post-exploitation objective of a successful CVE-2026-0250 attack and these are the most common persistence mechanisms at that privilege level. | Process memory dumps of PanGPA.exe and PanGPS.exe (captured via ProcDump: 'procdump -ma PanGPA.exe pangpa.dmp') from any endpoint suspected of connecting through a rogue or compromised network during the exposure window — heap corruption artifacts from the buffer overflow condition described in CVE-2026-0250 may be present in process memory and can confirm exploitation attempts even in the absence of other indicators.

Per-Action IR Details

Containment — Identify all endpoints running GlobalProtect App 6.0.x, 6.1.x, 6.2.x, or 6.3.x on Windows, macOS, Linux, Android, or ChromeOS, and GlobalProtect UWP App 6.3.x on Windows. Prioritize endpoints

that connect from untrusted or public networks (hotels, conferences, shared Wi-Fi) where network adjacency assumptions cannot be enforced. Restrict gateway access for unpatched clients if your GlobalProtect configuration supports enforcing minimum client versions. Source: Palo Alto Networks Security Advisory CVE-2026-0250.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST SC-7 (Boundary Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: On Windows, run: 'Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -like "*GlobalProtect*"} | Select-Object Name,Version,PSComputerName' across managed endpoints via PowerShell Remoting to extract version strings without SIEM. On macOS/Linux, query osquery with 'SELECT name, version FROM apps WHERE name LIKE "%GlobalProtect%";' or parse '/Applications/GlobalProtect.app/Contents/Info.plist' for CFBundleShortVersionString. For Android/ChromeOS, pull installed app versions via Android Debug Bridge (adb shell dumpsys package com.paloaltonetworks.globalprotect) or MDM console inventory export. Maintain a flat CSV of hostname, OS, GP version, and last-seen network SSID to prioritize mobile workers who regularly use public Wi-Fi.

Evidence: Before restricting gateway access, capture the GlobalProtect gateway authentication logs (PAN-OS Traffic and System logs) showing which client versions successfully authenticated and from which source IPs — specifically filter for clients sourced from non-corporate IP ranges (hotel DHCP blocks, Starlink, cellular NAT). On Windows endpoints, snapshot the GlobalProtect service process tree from Task Manager or via 'Get-Process -Name PanGPS,PanGPA | Select-Object Id,Name,Path,StartTime' to establish a baseline before any changes. Preserve the GlobalProtect client-side diagnostic log bundle (on Windows: C:\Program Files\Palo Alto Networks\GlobalProtect\PanGPA.log and PanGPS.log) as these record connection negotiation details that would reflect MitM-induced TLS anomalies prior to containment.

Detection — Query your endpoint management or MDM inventory for GlobalProtect App version strings matching 6.0.x, 6.1.x, 6.2.x, or 6.3.x (pre-patch). In SIEM, review GlobalProtect gateway logs for anomalous TLS negotiation failures or repeated connection resets from the same source, which may indicate MitM probe activity. No public IOCs are currently available; exploitation attempts would appear at the network layer before client-side logging triggers.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without SIEM, deploy Wireshark or tcpdump at the GlobalProtect gateway network perimeter and capture on the GlobalProtect SSL/TLS port (TCP 443 or UDP 4501 for IPsec) filtering for: 'tcp.flags.reset==1 && ip.dst==[gateway_IP]' to surface repeated RST storms indicative of MitM connection manipulation. On Windows endpoints, enable Sysmon with a configuration that captures Event ID 3 (Network Connection) for PanGPA.exe and PanGPS.exe processes — unexpected outbound TLS connections from these processes to non-Palo Alto infrastructure would be anomalous. Use the community Sigma rule framework to write a detection against Windows Security Event Log for Event ID 4688 (Process Creation) where ParentImage matches PanGPS.exe or PanGPA.exe and ChildImage is cmd.exe, powershell.exe, or any shell — this would indicate post-exploitation code execution under the SYSTEM context that CVE-2026-0250 enables.

Evidence: Before concluding no exploitation occurred, collect: (1) Full GlobalProtect gateway system logs from PAN-OS filtered for 'globalprotect' events in the exposure window (between client's last known clean state and patch date of May 13, 2026) — specifically auth failures, SSL handshake errors, and tunnel negotiation anomalies. (2) On Windows, query Windows Security Event Log for Event ID 4624 (Logon) with Logon Type 5 (Service) or Type 4 (Batch) where the Subject Account is SYSTEM and the logon time post-dates the endpoint's last GP connection from an untrusted network, which could reflect SYSTEM-level persistence established via the buffer overflow. (3) Capture

memory from the PanGPA.exe and PanGPS.exe processes using ProcDump ('procdump -ma PanGPA.exe pangpa.dmp') on any endpoint suspected of connecting through a compromised network — heap corruption artifacts from the buffer overflow may be recoverable before process restart.

Eradication — Apply the patches published by Palo Alto Networks on May 13, 2026, for all affected branches (6.0.x, 6.1.x, 6.2.x, 6.3.x). Obtain the updated installers directly from the Palo Alto Networks support portal at https://support.paloaltonetworks.com (official vendor portal; human validation recommended for specific build numbers). For Android and ChromeOS deployments, push updates via your MDM. Confirm iOS clients are unaffected and do not require action.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: For teams without an enterprise patch management platform, generate SHA-256 hashes of the Palo Alto-provided installers immediately after download from the support portal and verify against the vendor-published checksums before deployment — use 'certutil -hashfile GlobalProtect.msi SHA256' on Windows or 'sha256sum GlobalProtect.pkg' on macOS/Linux. Stage patched MSI or PKG installers on an internal file share and push via GPO Software Installation (Windows) or a simple shell script loop over SSH for Linux hosts ('for host in $(cat hosts.txt); do ssh $host "sudo installer -pkg GlobalProtect.pkg -target /"; done'). For Android devices without MDM, issue an advisory requiring manual update from the enterprise app store or the Palo Alto support portal and verify completion via the MDM compliance report or manual check-in log.

Evidence: Before deploying the patch, on any endpoint that connected from a high-risk untrusted network during the exposure window, run a full filesystem integrity check focused on directories where SYSTEM-level code execution would implant persistence: on Windows, check 'C:\Windows\System32\', 'C:\Windows\SysWOW64\', and 'C:\ProgramData\' for files with creation or modification timestamps post-dating the last known clean GP connection; use 'Get-ChildItem -Path C:\Windows\System32 -Recurse | Where-Object {$_.LastWriteTime -gt [datetime]"2026-04-01"} | Select-Object FullName,LastWriteTime' as a starting query. On macOS, run 'sudo find /Library/LaunchDaemons /Library/LaunchAgents /System/Library/LaunchDaemons -newer /var/log/system.log -ls' to detect persistence mechanisms installed at SYSTEM (root) level. Preserve these snapshots prior to patching, as the patch installer may overwrite GlobalProtect binaries that could otherwise be compared against known-good hashes.

Recovery — After patching, verify client version strings via endpoint management tooling to confirm all devices are running patched builds. Re-run your GlobalProtect gateway connection health checks to confirm normal TLS handshake behavior. Monitor gateway and endpoint logs for 48 to 72 hours post-patch for any anomalous connection patterns that may indicate prior exploitation attempts that went undetected.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-2 (Flaw Remediation), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-4 (Incident Handling), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Post-patch, re-run the PowerShell or osquery version inventory commands from the containment step and produce a diff against the pre-patch baseline CSV to confirm all previously vulnerable version strings are replaced. To validate TLS handshake normalization without a SIEM, use Wireshark to capture a GlobalProtect tunnel establishment from a test endpoint through the gateway and verify the Client Hello and Server Hello complete without RST or alert records — a clean handshake will show TLS 1.3 or 1.2 completion with no retransmission anomalies. For the 48–72 hour monitoring window, run a scheduled task every 6 hours using 'Get-EventLog -LogName Security -InstanceId 4688 -After (Get-Date).AddHours(-6) | Where-Object {$_.Message -like "*PanGP*"}' to catch any unexpected child processes spawned from GlobalProtect service processes, which would suggest a pre-patch compromise persisting through the patch cycle.

Evidence: During the recovery monitoring window, focus evidence collection on indicators of pre-patch compromise that would survive patching: (1) On Windows, query Scheduled Tasks for any entries created during the exposure window via 'Get-ScheduledTask | Where-Object {$_.Date -gt [datetime]"2026-04-01"} | Select-Object TaskName,TaskPath,Date' — SYSTEM-level code execution from CVE-2026-0250 exploitation would commonly establish scheduled task persistence. (2) Review Windows Registry Run keys ('HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' and 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon') for entries with timestamps in the exposure window. (3) On macOS, check LaunchDaemons in '/Library/LaunchDaemons/' for plist files created between initial exposure and patch date, as root-level execution would target this persistence path.

Post-Incident — Review whether your network segmentation and VPN architecture relies on adjacency assumptions that a MitM attacker could challenge (e.g., split-tunnel configurations, public Wi-Fi usage policies). Evaluate whether your GlobalProtect deployment enforces minimum client version at the gateway level; if not, this is a control gap to remediate. Document any endpoints that were slow to patch and apply a risk-based review of activity logs for those devices covering the exposure window.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity (Lessons Learned)

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: To assess split-tunnel exposure without enterprise tooling, extract GlobalProtect gateway configuration from PAN-OS and review the split-tunnel include/exclude route lists — if 'No Direct Access to Local Network' is not enforced, remote endpoints on public Wi-Fi are fully reachable by adjacent attackers during the connection window. Document this finding with the specific gateway name and policy name in your risk register. For the risk-based log review of slow-to-patch endpoints, pull the full GlobalProtect client diagnostic logs (Windows: 'C:\Program Files\Palo Alto Networks\GlobalProtect\PanGPA.log'; macOS: '/Library/Logs/PaloAlto/GlobalProtect/PanGPA.log') and grep for 'SSL' or 'TLS' error strings during the exposure window to identify any anomalous negotiation events that preceded exploitation: 'Select-String -Path "C:\Program Files\Palo Alto Networks\GlobalProtect\PanGPA.log" -Pattern "SSL|TLS|error|failed" | Where-Object {$_.Line -match "2026-0[4-5]-"}'.

Evidence: For the post-incident review, reconstruct the full exposure window for each slow-to-patch endpoint by correlating: (1) GlobalProtect gateway authentication logs showing the endpoint's connection history, source IP geolocation, and network type (corporate vs. non-corporate CIDR) from first vulnerable version detection to patch confirmation date. (2) Any EDR or Sysmon telemetry from the endpoint covering SYSTEM-context process creation (Event ID 4688 with elevated integrity level) during sessions that originated from public or untrusted networks — this is the highest-fidelity signal for successful CVE-2026-0250 exploitation given its SYSTEM-level code execution outcome. (3) Network flow data (NetFlow or firewall session logs) from the GlobalProtect gateway showing the tunnel source IPs for affected endpoints — sessions originating from known conference or hotel IP ranges during the exposure window should be flagged for deeper forensic review.

Detection Guidance

No public IOCs or exploit code are available as of this writing. Detection focuses on inventory and version verification rather than behavioral indicators at this stage. Query endpoint management, MDM, or SIEM asset inventory for GlobalProtect App versions matching 6.0.x, 6.1.x, 6.2.x, or 6.3.x. In network logs, look for anomalous TLS handshake failures or TCP resets on GlobalProtect Portal/Gateway ports (default: 443) originating from adjacent network segments or unusual source IPs. Because exploitation requires MitM positioning, correlate any suspicious network anomalies with physical location data for the affected endpoint (e.g., travel to conference, hotel, or public Wi-Fi). Post-exploitation, look for SYSTEM-level process creation

events on Windows endpoints (Event ID 4688 with elevated integrity level) initiated by GlobalProtect process lineage. Monitor NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-0250) and Palo Alto Networks advisories for updated EPSS scores and any reported exploitation.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1068** — Exploitation for Privilege Escalation
- **T1203** — Exploitation for Client Execution
- **T1557** — Adversary-in-the-Middle

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

OWASP-TOP10-2021

- **A03:2021** — Injection

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

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
T1190	Exploit Public-Facing Application	Initial-Access
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1203	Exploitation for Client Execution	Execution
T1557	Adversary-in-the-Middle	Credential-Access

Sources

Source	URL	Tier
Palo Alto Networks Security Advisories	https://security.paloaltonetworks.com/CVE-2026-0250	T3
CVE Record: CVE-2026-0250 - Palo Alto Networks, Inc.	https://www.cve.org/CVERecord?id=CVE-2026-0250	T3
CVE-2026-0250 — Memory Corruption in Globalprotect App+1 | dbugs	https://dbugs.ptsecurity.com/vulnerability/PT-2026-40751	T3
Palo Alto Defender's Guide Refutes Mythos Claim - flyingpenguin	https://www.flyingpenguin.com/palo-alto-defenders-guide-refutes-myt...	T3
RHSA-2026:0250 - Security Advisory - Red Hat Customer Portal	https://access.redhat.com/errata/RHSA-2026:0250	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-0250	T1

Generated 2026-05-14 06:53 UTC by TJS Security Command Center