INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-04 06:48 UTC

CVE-2025-0108: Palo Alto PAN-OS GlobalProtect Auth Bypass Under Active Exploitation

CVE VULNERABILITY | CRITICAL | CVSS 9.1

SCC Item ID	SCC-CVE-2026-0263
Type	CVE Vulnerability
CVE ID	CVE-2025-0108
Severity	CRITICAL
CVSS Base Score	9.1
EPSS Score	0.9412 (100th percentile)
Affected Products	Palo Alto Networks PAN-OS (GlobalProtect web management interface); specific affected versions per Palo Alto Security Advisory CVE-2025-0108
Published	2 days ago
Discovery Source	Serper

Executive Summary

CVE-2025-0108 is a critical authentication bypass flaw in Palo Alto Networks PAN-OS affecting the GlobalProtect VPN web management interface, with a CVSS base score of 9.1 and an EPSS score of 0.94 (99.9th percentile exploitation likelihood). Unauthenticated attackers can bypass access controls on exposed management interfaces, and confirmed active exploitation has been observed across multiple attack waves. Organizations running affected PAN-OS versions with internet-accessible management interfaces face immediate risk of unauthorized network access, lateral movement into corporate infrastructure, and potential compromise of VPN-protected systems.

Technical Analysis

CVE-2025-0108 is an authentication bypass vulnerability (CWE-306: Missing Authentication for Critical Function) in the PAN-OS web management interface used by the GlobalProtect VPN gateway. CVSS base score: 9.1 (CVSS:3.1 vector pending NVD publication). EPSS: 0.941 (99.9th percentile). The flaw maps to MITRE ATT&CK T1190 (Exploit Public-Facing Application) and T1078 (Valid Accounts), indicating post-exploitation pivot potential through hijacked session context. Active exploitation has been confirmed in multiple attack waves. Exploitation requires network reachability to the management interface; internet-exposed management planes are highest risk. Palo Alto Networks has issued a security advisory at https://security.paloaltonetworks.com/CVE-2025-0108 with affected version specifics and patch guidance. NVD

entry: https://nvd.nist.gov/vuln/detail/CVE-2025-0108. Source reliability for this item is moderate; confirm version-specific impact against the Palo Alto advisory directly before deploying patches.

Action Checklist

1. Step 1: Containment, Immediately restrict access to the PAN-OS web management interface. Per Palo Alto best practice, the management interface should never be internet-facing; if it is, block external access at the perimeter firewall now. Verify no public IPs resolve to the management plane. Reference: Palo Alto Networks security advisory https://security.paloaltonetworks.com/CVE-2025-0108. Apply NIST 800-53 AC-17 (Remote Access) and ensure management interface segmentation per CIS Controls v8 3 (Address Authorized Software).
2. Step 2: Detection, Query firewall and web server access logs for unauthenticated HTTP/HTTPS requests to the GlobalProtect management interface that resulted in 200 or 302 responses; these may indicate successful bypass. Look for access to authenticated management endpoints (/php/, /api/) from external IPs without preceding valid session tokens. Cross-reference source IPs against threat intelligence feeds. Per NIST CSF DE.AE-3 (Detect > Analysis & Evaluation), review and analyze audit records for anomalous access patterns. If a SIEM is in use, build a detection rule scoped to management interface URIs with no valid prior authentication event. Monitor for unexpected management interface access events correlated with account activity.
3. Step 3: Eradication, Apply the patch specified in the Palo Alto Networks security advisory https://security.paloaltonetworks.com/CVE-2025-0108 for your specific PAN-OS version. Consult the advisory's affected version table to confirm your version and the corresponding fixed release. Do not rely on version assumptions; verify the installed version against the advisory. Reference CIS Controls v8 2 (Software Asset Management) and NIST 800-53 SI-2 (Flaw Remediation).
4. Step 4: Recovery, After patching, verify the management interface responds only to authenticated sessions. Rotate credentials for any accounts that had access to the management interface per NIST 800-53 AC-2 (Account Management). Audit active sessions and terminate any sessions that originated during the exploitation window. Re-enable management interface access only from trusted, restricted IP ranges per AC-17 (Remote Access). Monitor audit logs for 72 hours post-patch for residual anomalous activity.
5. Step 5: Post-Incident, Conduct a control gap review against NIST 800-53 AC-6 (Least Privilege) and AC-17 (Remote Access) to assess whether management interfaces are properly segmented from internet-facing networks. Document findings and update network segmentation policies. Implement password hardening and multi-factor authentication for all management plane accounts per NIST 800-53 AC-2 (Account Management). Review GlobalProtect configuration baseline against CIS Controls v8 1 (Governance & Risk Management). If exploitation is confirmed, escalate to incident response and investigate for lateral movement.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO and legal/compliance immediately if log evidence confirms successful unauthenticated access to the PAN-OS management interface (HTTP 200/302 responses to /php/ or /api/ from external IPs), if configuration changes are detected during the exploitation window indicating attacker-initiated modifications, or if the management VLAN has lateral connectivity to systems in scope for PCI-DSS, HIPAA, or other regulated data environments requiring breach notification assessment.
Recovery Notes	After patching to the fixed PAN-OS release per the CVE-2025-0108 advisory, validate remediation by testing authentication enforcement on the management interface from an external IP and confirming all previously active sessions have been terminated and credentials rotated. Monitor PAN-OS System and Traffic logs continuously for 72 hours post-patch, specifically watching for any recurrence of unauthenticated 200/302 responses to /php/ or /api/ URIs, anomalous admin account activity, or unexpected outbound connections from the management plane. If exploitation was confirmed, extend lateral movement investigation to all network segments reachable from the management VLAN before declaring the incident closed.
Forensic Artifacts	PAN-OS Monitor > Logs > Traffic: HTTP 200 or 302 responses to URIs matching /php/ or /api/ from non-RFC1918 source IPs during the exploitation window — primary indicator of successful CVE-2025-0108 auth bypass | PAN-OS Monitor > Logs > System: Authentication events (AUTH-SUCCESS, AUTH-FAILURE) and admin session creation records from external IPs, cross-referenced against known admin source IP allowlist to identify unauthorized management plane access | PAN-OS configuration audit log (`show config audit`): Any configuration changes — firewall rule additions, new admin account creation, certificate exports, or GlobalProtect gateway/portal modifications made during the exploitation window that indicate attacker-initiated changes post-bypass | Management interface web server access logs (nginx/Apache logs under /var/log/ on the PAN-OS filesystem, if accessible): Raw HTTP request logs showing full URI paths, source IPs, HTTP methods, response codes, and session cookie values — critical for reconstructing exact bypass request sequences and identifying any PHP web shell upload attempts | Network flow data (NetFlow/IPFIX/sFlow) from the management VLAN segment: East-west connection records from the firewall management IP to internal hosts during and after the exploitation window, used to identify post-exploitation lateral movement consistent with MITRE ATT&CK T1190 follow-on TTPs

Per-Action IR Details

Step 1: Containment — Immediately restrict access to the PAN-OS web management interface. Per Palo Alto best practice, the management interface should never be internet-facing; if it is, block external access at the perimeter firewall now. Verify no public IPs resolve to the management plane. Reference: Palo Alto Networks security advisory CVE-2025-0108 (security.paloaltonetworks.com/CVE-2025-0108). NIST AC-17 (Remote Access) and CIS 4.4 (Implement and Manage a Firewall on Servers) apply here.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Run `curl -sk https:///php/` from an external IP — a 200 or redirect response confirms the management interface is reachable externally and must be blocked immediately. On the upstream perimeter device, apply an ACL or iptables rule (e.g., `iptables -I INPUT -p tcp --dport 443 -s 0.0.0.0/0 -j DROP` with exceptions for admin IP ranges) to block all non-approved source IPs to the PAN-OS management plane. Use `nmap -p 443,4443 --script http-title ` to confirm the interface is no longer externally reachable after the block is applied.

Evidence: Before restricting access, capture current network state: run `netstat -an` or `ss -tlnp` on any jump host with visibility to the management VLAN to document active connections to PAN-OS management ports (TCP 443, 4443). Export the PAN-OS Traffic and System logs via CLI (`scp export log traffic ...`) covering the 30-day window prior to discovery, paying specific attention to source IPs that reached the management plane. Screenshot or export the Palo Alto 'Monitor > Logs > System' entries showing authentication events and any GLOBALPROTECT log entries showing unexpected session initiation without credential validation. Preserve the raw PAN-OS running config (`show config running`) to establish a pre-remediation baseline for later integrity comparison.

Step 2: Detection — Query firewall and web server access logs for unauthenticated HTTP/HTTPS requests to the GlobalProtect management interface that resulted in 200 or 302 responses — these may indicate successful bypass. Look for access to authenticated management endpoints (/php/, /api/) from external IPs without preceding valid session tokens. Cross-reference source IPs against threat intelligence feeds. Per AU-6, review and analyze audit records for anomalous access patterns. If a SIEM is in use, build a detection rule scoped to management interface URIs with no valid prior authentication event. Apply D3-LAM (Local Account Monitoring) to identify any account activity following unexpected management interface access.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST AU-2 (Event Logging), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use grep or awk directly against PAN-OS exported traffic and system logs: `grep -E '(/php/|/api/)' pan_traffic.log | grep -E ' 200 | 302 ' | grep -v 'authn_success'` to surface unauthenticated hits against authenticated endpoints. Convert PAN-OS logs to CSV via `scp export log traffic ... format csv` and import into a spreadsheet to pivot on source IP and URI path. Cross-reference attacker IPs against free threat intel sources (AbuseIPDB API: `curl https://api.abuseipdb.com/api/v2/check?ipAddress=`, or grep against the CISA Known Exploited Vulnerabilities feed). Deploy Zeek or Wireshark on a span port to capture live HTTP/HTTPS metadata to the management interface and inspect for requests to `/php/` or `/api/` lacking `PHPSESSID` or equivalent valid session cookies.

Evidence: Collect PAN-OS 'Monitor > Logs > System' entries for event type AUTH-FAILURE or any AUTH event originating from external (non-RFC1918) IPs targeting the management interface. Export 'Monitor > Logs > Traffic' filtered on destination zone 'mgmt' and destination port 443 or 4443 — specifically HTTP 200/302 responses to URIs matching `/php/` or `/api/` from sources with no prior valid authentication sequence. Pull PAN-OS 'Monitor > Logs > GlobalProtect' for anomalous gateway or portal session creation events that lack corresponding credential-validation log entries. If the management interface had web server access logging enabled, export the underlying nginx or Apache access logs (path varies by PAN-OS version, typically under `/var/log/`) and search for POST requests to PHP endpoints from unauthenticated sessions.

Step 3: Eradication — Apply the patch specified in the Palo Alto Networks security advisory CVE-2025-0108 for your specific PAN-OS version. Consult the advisory's affected version table to confirm your version and the corresponding fixed release. Do not rely on version assumptions — verify the installed version against the advisory. Reference CIS 7.3 (Perform Automated Operating System Patch Management) and NIST SI-2 (Flaw Remediation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), NIST SA-10 (Developer Configuration Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Before patching, verify exact PAN-OS version via CLI: `show system info | match sw-version` and map it against the Palo Alto CVE-2025-0108 advisory version table to confirm the correct target release. Take a full configuration backup via `scp export configuration from running-config.xml to ` before applying any update. After patching, re-run `show system info | match sw-version` to confirm the new version installed successfully. Validate the fix by attempting to replicate the bypass condition from a test external IP: a properly patched system should return

HTTP 401 or 403 on unauthenticated requests to `/php/` and `/api/` endpoints rather than 200 or 302.

Evidence: Before applying the patch, preserve a forensic snapshot: export the full PAN-OS running configuration (`show config running`), current active administrator sessions (`show admins`), and the system log covering the exploitation window (`scp export log system ...`). Capture a hash (SHA-256) of key PAN-OS system binaries if accessible via the management CLI to establish a pre-patch integrity baseline. Document the exact installed version, serial number, and any custom PHP files or management interface customizations that could indicate attacker-planted persistence (web shells dropped to the management interface via the auth bypass are a documented post-exploitation technique for this CVE class).

Step 4: Recovery — After patching, verify the management interface responds only to authenticated sessions. Rotate credentials for any accounts that had access to the management interface (D3-CRO: Credential Rotation). Audit active sessions and terminate any sessions that originated during the exploitation window. Re-enable management interface access only from trusted, restricted IP ranges per AC-17. Monitor AU-6 logs for 72 hours post-patch for residual anomalous activity.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-17 (Remote Access), NIST AC-2 (Account Management), NIST AC-12 (Session Termination), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Terminate all active management sessions via PAN-OS CLI: `clear admin-sessions` followed by `show admins` to confirm no residual sessions remain. Force credential rotation for all local admin accounts: `set mgt-config users password` for each account in `show mgt-config users`. For 72-hour post-patch monitoring without a SIEM, schedule a cron job or Windows Task Scheduler entry to run every 15 minutes pulling `show log system direction equal forward` and piping output to a local log file, then use `grep -i 'auth\|login\|admin\|config'` to surface anomalous activity. Test authentication enforcement by attempting a curl request to `/php/` from an external IP — confirmed patched systems must return 401/403, not 200/302.

Evidence: Before rotating credentials and terminating sessions, export `show admins` output and `show log system` entries covering all sessions active during the exploitation window — these are key forensic artifacts establishing which accounts (if any) were accessed or modified via the bypass. Capture `show config audit` to identify any configuration changes made during the exploitation window that may indicate attacker-initiated changes (firewall rule additions, admin account creation, certificate exports). Preserve these exports with timestamps and chain of custody documentation before any recovery actions alter the system state.

Step 5: Post-Incident — Conduct a control gap review against AC-6 (Least Privilege) and AC-17 (Remote Access) to assess whether management interfaces are properly segmented from internet-facing networks. Document findings and update network segmentation policies. Implement D3-CH (Credential Hardening) for all management plane accounts. Review GlobalProtect configuration baseline against CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure). If exploitation is confirmed, treat as an incident and follow your IR playbook for potential lateral movement investigation.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), NIST CA-7 (Continuous Monitoring), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Conduct the management interface segmentation review using free network scanning: run `nmap -sV -p 443,4443,8443 --open ` from an external vantage point (or use Shodan's free tier querying your ASN) to identify any PAN-OS management interfaces still exposed. For lateral movement investigation following confirmed exploitation, deploy Sysmon (config targeting process creation, network connections, and file writes) on Windows endpoints reachable from the firewall management VLAN and hunt for MITRE ATT&CK T1190 (Exploit Public-Facing Application) follow-on TTPs including T1078 (Valid Accounts) and T1059 (Command and Scripting Interpreter). Write a Sigma rule targeting web server logs for POST requests to PAN-OS management URIs from non-RFC1918 addresses to

operationalize detection going forward.

Evidence: For confirmed exploitation, collect and preserve: all PAN-OS system and traffic logs from the full exploitation window (minimum 30 days prior to detection), any configuration diff output from `show config audit` showing changes made during the window, network flow data (NetFlow/IPFIX if available) showing east-west traffic from the management VLAN to internal segments that could indicate post-exploitation lateral movement, and DNS query logs from the firewall management interface for any outbound resolution requests that could indicate C2 beaconing initiated from the management plane. If a web shell was planted via the auth bypass, look for anomalous PHP file creation or modification timestamps in the PAN-OS management interface web root.

Detection Guidance

Primary detection focus: unauthenticated access to the PAN-OS web management interface. Query web server and PAN-OS traffic logs for HTTP 200 or 302 responses to management-plane URIs (/php/, /api/, /esp/) originating from external or unexpected source IPs with no valid session authentication event preceding the request. Flag any management interface access from IPs not in your approved management access allowlist. In your SIEM, correlate PAN-OS management access logs against your firewall allow rules; any management session established from a non-allowlisted IP is a high-priority alert. Monitor for modifications to configuration files or authentication mechanisms on the PAN-OS management plane following suspicious access. As of this publication, Palo Alto Networks and CISA have not released a public IOC list. Monitor official channels (https://security.paloaltonetworks.com and https://cisa.gov) for IOC publication; do not rely on unverified IOCs from social media or third-party forums.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://nvd.nist.gov/vuln/detail/CVE-2025-0108`	NVD authoritative entry for CVE-2025-0108 — verified T1 source	HIGH

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1078** — Valid Accounts

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-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)

- **IA-5** — Authenticator Management
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

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
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
	https://www.darkreading.com/threat-intelligence/patch-palo-alto-aut...	T3
Patch Now: Another Palo Alto Auth Bypass Bug Under Active Exploit	https://x.com/TheCyberSecHub/status/2061464338624586213	T3
Palo Alto GlobalProtect VPN auth bypass flaw now exploited in ...	https://www.reddit.com/r/paloaltonetworks/comments/1tsja1c/palo_alt...	T3

Source	URL	Tier
Patch Now: Palo Alto Auth Bypass Bug Under Active Exploit	https://www.facebook.com/darkreadingcom/posts/patch-now-another-pal...	T3
CVE-2025-0108 PAN-OS: Authentication Bypass in the ...	https://security.paloaltonetworks.com/CVE-2025-0108	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-0108	T1

Generated 2026-06-04 06:48 UTC by TJS Security Command Center