INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 08:40 UTC

Unauthenticated RCE Zero-Day CVE-2026-0300 Under Active Exploitation in PAN-OS Firewalls, No Patch Available

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0125
Type	CVE Vulnerability
CVE ID	CVE-2026-0300
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Palo Alto Networks PAN-OS, PA-Series and VM-Series firewalls (User-ID Authentication Portal / Captive Portal)
Published	2026-05-06T05:18:16
Discovery Source	Rss

Executive Summary

Palo Alto Networks has disclosed CVE-2026-0300, a critical unauthenticated remote code execution zero-day in PAN-OS firewalls, currently under active exploitation with no patch available. Attackers can gain root-level control of internet-exposed PA-Series and VM-Series firewalls without any credentials, bypassing perimeter security entirely. Organizations with internet-facing Palo Alto firewalls face immediate risk of network compromise, lateral movement, and data exfiltration until mitigations are applied.

Technical Analysis

CVE-2026-0300 is a buffer overflow vulnerability (CWE-120, CWE-121) with a possible OS command injection component (CWE-78) in the PAN-OS User-ID Authentication Portal and Captive Portal. Affected products: PA-Series and VM-Series firewalls running PAN-OS (specific version ranges TBD, pending official vendor advisory). Attack vector is network-accessible, unauthenticated, requiring no user interaction. Exploitation achieves root-level remote code execution on the firewall itself. CVSS base score: 9.5 (Critical). Vendor CVSS score pending from Palo Alto Networks. No patch is currently available. Active exploitation is confirmed per CSA Singapore advisory AL-2026-048 (see sources) and secondary reporting from BleepingComputer and SecurityWeek. Exposure estimate (5,800 VM-Series instances) is reported in secondary sources; verify primary source and methodology for operational decision-making. MITRE ATT&CK techniques observed or applicable:

T1190 (Exploit Public-Facing Application), T1068 (Exploitation for Privilege Escalation), T1505.003 (Server Software Component: Web Shell), T1133 (External Remote Services), T1059 (Command and Scripting Interpreter). Attribution is not established. Confidence note: Technical details (CVSS vector, exact version ranges) are medium confidence pending NVD and vendor advisory publication. Active exploitation status is high confidence per CSA Singapore T1 source. Verify version applicability and mitigation steps against official Palo Alto Networks advisory before operational deployment.

Action Checklist

1. Containment, immediately disable or restrict internet access to the PAN-OS User-ID Authentication Portal and Captive Portal interfaces on all PA-Series and VM-Series firewalls; place these management interfaces behind a VPN or restrict to known IP ranges. Pending vendor guidance, disable these portals via device configuration menu if possible.
2. Detection, audit firewall logs for anomalous authentication portal activity: unexpected POST requests, oversized input fields, or process spawning from the User-ID or Captive Portal service; check for new or modified files in web-accessible directories; review for unexpected outbound connections from the firewall management plane; monitor for indicators consistent with T1505.003 (web shell activity) and T1059 (unexpected command interpreter execution).
3. Eradication, no vendor patch is available as of this item's publication date. Monitor the Palo Alto Networks Security Advisories page (security.paloaltonetworks.com) for patch and compensating control guidance. Implement network-based compensating controls immediately: disable User-ID and Captive Portal services if not required for operations, or restrict access to trusted IP ranges only.
4. Recovery, once a patch is released, apply it to all affected PA-Series and VM-Series instances immediately; after patching, conduct full integrity checks on firewall configurations, routing tables, and authentication settings; review for signs of persistence mechanisms (new admin accounts, modified configurations, unexpected scheduled tasks or scripts); restore from a known-good configuration backup only after confirming no compromise occurred.
5. Post-Incident, audit internet-exposure footprint for all security appliances and implement a policy prohibiting management or authentication portal interfaces from being internet-accessible without authentication gating; review segmentation between firewall management plane and production network; add this CVE class (unauthenticated RCE on perimeter security devices) to tabletop exercise scenarios.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and external IR retainer immediately if any of the following are confirmed: evidence of successful RCE (unexpected processes, web shells, or new accounts on the firewall), outbound C2 connections from the management plane, lateral movement into internal network segments reachable from the firewall's trusted interfaces, or if the affected firewalls protect environments subject to PCI DSS, HIPAA, or state breach notification laws — as unauthenticated root-level access to a perimeter device constitutes a presumptive breach trigger under most regulatory frameworks.

Recovery Notes	Do not restore portal functionality until the official Palo Alto Networks patch for CVE-2026-0300 has been applied and post-patch integrity verification of /var/appweb/ and /opt/pancfg/ confirms no residual web shells or modified binaries. After recovery, monitor PAN-OS system logs and management plane outbound connections continuously for a minimum of 30 days for delayed persistence activation (T1505.003 web shells with dormant callbacks or T1053 scheduled task execution) — given this is an active exploitation campaign, assume re-targeting is likely. Verify all firewall admin account MFA settings and rotate all local admin credentials on affected units before returning to production, as credential harvesting from the management plane is a likely second-stage objective following unauthenticated RCE.
Forensic Artifacts	PAN-OS SSL/VPN and Captive Portal web access logs at /var/log/pan/sslvpn* — will contain HTTP POST requests with oversized or malformed payloads to /php/login.php or /ssl-vpn/login.esp that represent exploit delivery attempts for CVE-2026-0300 | PAN-OS management server process logs at /var/log/pan/ms.log and /var/log/pan/system — will record unexpected child process spawning from mgmtsrvr or useridd if the RCE payload executed successfully (T1059 — Command and Scripting Interpreter) | Filesystem modification timestamps in /var/appweb/ and /opt/pancfg/ — attacker-dropped web shells (T1505.003) following successful exploitation would appear as PHP or Lua files with creation/modification timestamps correlating to the exploit attempt window | PAN-OS running configuration export (running-config.xml) and admin account listing from `show admins all` — post-exploitation persistence via T1136 (Create Account) would manifest as undocumented local admin accounts or modified authentication profiles not present in the pre-incident configuration baseline | Network flow records or firewall traffic logs showing unexpected outbound connections from the management plane IP to external destinations — successful RCE enabling a reverse shell or C2 beacon (T1071 — Application Layer Protocol) from the firewall's management interface would appear as anomalous initiated sessions to non-allowlisted external IPs on ports 443, 80, or high ephemeral ports

Per-Action IR Details

Containment — immediately disable or restrict internet access to the PAN-OS User-ID Authentication Portal and Captive Portal interfaces on all PA-Series and VM-Series firewalls; place these management interfaces behind a VPN or restrict to known IP ranges per Palo Alto Networks guidance; consult the official Palo Alto Networks Security Advisory for interface-specific disable procedures.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Without enterprise NAC or automated orchestration: log into each PA-Series/VM-Series management console and navigate to Device > Setup > Interfaces; disable the Authentication Portal and Captive Portal bindings on all internet-facing interfaces immediately. On the perimeter router or upstream ACL, block TCP/443 and TCP/8080 (or whichever ports your portal is bound to) inbound from 0.0.0.0/0 to the firewall's external IP, permitting only your documented administrative IP ranges. Document each change with a timestamp and the admin account used. If using Panorama, push an emergency Security Policy rule blocking inbound access to portal URLs (/php/login.php, /ssl-vpn/login.esp) from any source.

Evidence: Before restricting access, capture a full netstat or 'show system state' snapshot from the PAN-OS CLI (`debug system state dump`) to record active sessions on the portal interfaces. Export the current running configuration (`show config running`) as a pre-containment baseline. Pull web server access logs from /var/log/pan/gp* and /var/log/pan/sslvpn* to preserve evidence of pre-containment exploit attempts targeting the User-ID and Captive Portal endpoints.

Detection — audit firewall logs for anomalous authentication portal activity: unexpected POST requests, oversized input fields, or process spawning from the User-ID or Captive Portal service; check for new or modified files in web-accessible directories; review for unexpected outbound connections from the firewall management plane; monitor for indicators consistent with T1505.003 (web shell activity) and T1059 (unexpected command interpreter execution).

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-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM: run the following directly on the PAN-OS management plane via SSH — `grep -E 'POST .*(login|portal|userid)' /var/log/pan/sslvpn*` to identify oversized or malformed POST bodies to the Captive Portal. To detect T1059 (unexpected command interpreter) spawned by the portal service, check `/var/log/pan/system` for entries referencing unexpected child processes of the User-ID daemon (useridd) or the web-facing process (mgmtsrvr). For T1505.003 web shell detection, run `find /opt/pancfg/mgmt/panos-configs/ /var/appweb/ -name '*.php' -newer /var/svc/panos_version -ls` to find files written after last known-good state. For unexpected outbound connections from the management plane, run `netstat -an | grep ESTABLISHED` and cross-reference against your allowlisted management destinations.

Evidence: Capture PAN-OS traffic logs filtered for the User-ID Authentication Portal and Captive Portal service IPs before any log rotation occurs — export via `tftp export log traffic` or via Panorama log export. Collect /var/log/pan/sslvpn*, /var/log/pan/system, and /var/log/pan/ms.log in their entirety. Document any process listing from `show system resources` and `debug software restart process management-server` output showing abnormal CPU/memory spikes on the management plane process that correlate with inbound portal requests.

Eradication — no vendor patch is available as of this item's publication date; apply any compensating controls published in the official Palo Alto Networks advisory (such as disabling affected portal features via device configuration); monitor the Palo Alto Networks Security Advisories page for patch release; subscribe to PSIRT notifications at security.paloaltonetworks.com.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST CM-6 (Configuration Settings), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: While no patch exists: disable User-ID and Captive Portal features entirely via Device > User Identification > disable, and under Network > GlobalProtect > Portals remove any Captive Portal configurations — document each step. Set a daily calendar alert to check https://security.paloaltonetworks.com for CVE-2026-0300 advisory updates. If the portal cannot be fully disabled due to operational need, restrict the service to a non-routable management VLAN immediately and enforce an emergency change freeze on the affected firewalls. Use YARA rules targeting web shell signatures (e.g., the public YARA ruleset from CISA or VirusTotal community) scanned against /var/appweb/ and /opt/pancfg/ directories to confirm no persistent implant was dropped prior to containment.

Evidence: Before disabling portal features, capture a full configuration export (`scp export configuration from running-config.xml`) as forensic evidence of the pre-eradication state. If a web shell or implant is suspected (per T1505.003 detection results), collect a memory image of the management plane process using `/opt/panlogs/tech_support_logs` dump and preserve it offline before any service restarts. Hash all files in /var/appweb/ and /opt/pancfg/ using `find / -xdev -type f -exec md5sum {} \;` and compare against a known-good hash baseline from an uncompromised unit of the same PAN-OS version.

Recovery — once a patch is released, apply it to all affected PA-Series and VM-Series instances immediately; after patching, conduct full integrity checks on firewall configurations, routing tables, and authentication settings; review for signs of persistence mechanisms (new admin accounts, modified configurations, unexpected scheduled tasks or scripts); restore from a known-good configuration backup only after

confirming no compromise occurred.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), NIST IR-4 (Incident Handling), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: After Palo Alto Networks releases a patch for CVE-2026-0300: apply it via Device > Software > Check Now on each unit, or stage through Panorama using the software upgrade workflow. Post-patch, audit admin accounts by running `show admins all` on the PAN-OS CLI and cross-referencing against your documented admin inventory — remove any accounts not in the baseline (T1136 — Create Account). Check routing tables with `show routing route` for unauthorized static routes that could redirect traffic to an attacker-controlled hop. For unauthorized scheduled tasks or scripts (T1053), inspect `/var/svc/cron/` and `/etc/cron.d/` directories. Restore configuration from a pre-incident backup only after confirming its hash matches your documented pre-compromise backup.

Evidence: Before applying the patch, capture a final forensic snapshot: export full tech support file (`scp export tech-support`) which includes logs, system state, and configuration. Document the exact PAN-OS software version string (`show system info | match sw-version`) on each device as evidence of the vulnerable version run duration. After patching, re-run the file integrity check against /var/appweb/ and /opt/pancfg/ comparing to the post-patch known-good manifest provided or derivable from a freshly imaged unit of the same version, to confirm no attacker-planted files survived the upgrade.

Post-Incident — audit internet-exposure footprint for all security appliances and implement a policy prohibiting management or authentication portal interfaces from being internet-accessible without authentication gating; review segmentation between firewall management plane and production network; add this CVE class (unauthenticated RCE on perimeter security devices) to tabletop exercise scenarios.

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 SC-7 (Boundary Protection), NIST RA-3 (Risk Assessment), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For a 2-person team with no enterprise ASM tooling: use Shodan CLI (`shodan search 'http.title:"Palo Alto" org:"YOUR-ORG-ASN"`) or a free Shodan account web query to enumerate any remaining internet-exposed PAN-OS portal interfaces across your IP ranges. Document findings in a simple spreadsheet tracking each appliance, its external IP, whether the portal is exposed, and remediation status. Draft a one-page policy addendum requiring all new firewall deployments to have management and portal interfaces validated against a 'no direct internet exposure' checklist before go-live, signed by the CISO or delegate. Submit the unauthenticated RCE on perimeter device scenario to your next quarterly tabletop with a focus on detection lag and out-of-band management access.

Evidence: Compile the full incident timeline from log exports collected during detection and eradication phases, including the earliest evidence of exploit attempts in /var/log/pan/sslvpn* against the portal endpoints. Document the exposure window — time from CVE-2026-0300 public disclosure to portal restriction — as this determines breach notification obligation scope. Preserve all forensic artifacts (config exports, tech support files, file integrity reports, memory dumps) in a read-only evidence repository with chain-of-custody documentation per NIST IR-5 (Incident Monitoring) requirements.

Detection Guidance

Focus detection on the PAN-OS User-ID Authentication Portal and Captive Portal services. Review PAN-OS system logs and traffic logs for: abnormal or oversized HTTP/HTTPS requests to /php/login.php, /ssl-vpn/login.esp, or Captive Portal endpoints; process execution events spawned from web service processes

(indicative of CWE-78 command injection); unexpected outbound network connections from the firewall data or management plane to external IPs; creation of new files in web-accessible directories (web shell indicator, T1505.003); new local administrator accounts or changes to existing admin credentials. If you have SIEM integration with PAN-OS syslog, alert on process execution from the pan_task or Pan_ctd process families that do not match baseline. Cross-reference any suspicious source IPs against threat intelligence feeds. No confirmed public IOCs are available in sourced materials at time of publication, treat any anomalous portal activity as suspicious until ruled out.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs published in available sources at time of item creation`	Attribution is not established; no IP, domain, hash, or URL indicators have been confirmed in sourced materials. Monitor Palo Alto Networks Threat Intelligence and CISA for IOC releases.	LOW

Framework Mappings

MITRE-ATTACK

- **T1505.003** — Web Shell
- **T1068** — Exploitation for Privilege Escalation
- **T1190** — Exploit Public-Facing Application
- **T1133** — External Remote Services
- **T1059** — Command and Scripting Interpreter

NIST-800-53R5

- **CM-2** — Baseline Configuration
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

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

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
T1505.003	Web Shell	Persistence
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1190	Exploit Public-Facing Application	Initial-Access
T1133	External Remote Services	Persistence
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/palo-alto-networks-w...	T3
Palo Alto Networks to Patch Zero-Day Exploited to Hack Firewalls	https://www.securityweek.com/palo-alto-networks-to-patch-zero-day-e...	T3
Unauthenticated RCE in Palo Alto PAN-OS Actively Exploited	https://threatlandscape.io/blog/zero-day-cve-2026-0300-palo-alto-pa...	T3

Source	URL	Tier
Active Exploitation of Palo Alto Networks PAN-OS software	https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-048/	T1
CVE-2026-0300 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-0300	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-0300	T1

Generated 2026-05-06 08:40 UTC by TJS Security Command Center