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

PAN-OS Authentication Bypass via Cloud Authentication Service: Broad Version Exposure, Patches Partially Pending

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0176
Type	CVE Vulnerability
CVE ID	CVE-2026-0265
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Palo Alto Networks PAN-OS 10.2, 11.1, 11.2, 12.1, PA-Series firewalls, VM-Series firewalls, Panorama (virtual and M-Series appliances); Cloud NGFW and Prisma Access are NOT affected
Published	2026-05-13T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

A high-severity authentication bypass vulnerability in Palo Alto Networks PAN-OS allows an unauthenticated remote attacker to take full control of affected firewalls and Panorama management platforms without any credentials. PA-Series and VM-Series firewalls running PAN-OS 10.2, 11.1, 11.2, or 12.1 with Cloud Authentication Service enabled on a network-reachable interface are at risk. Patches are partially pending across all affected branches; organizations should apply available hotfixes immediately and restrict interface access where patches are not yet available.

Technical Analysis

CVE-2026-0265 is an authentication bypass in Palo Alto Networks PAN-OS affecting versions 10.2, 11.1, 11.2, and 12.1 on PA-Series firewalls, VM-Series firewalls, and Panorama (virtual and M-Series appliances). The vulnerability is exploitable only when the Cloud Authentication Service is enabled on a network-reachable management interface. An unauthenticated remote attacker can bypass authentication controls with no privileges required, yielding full confidentiality, integrity, and availability impact (CIA triad compromised). Root cause is mapped to CWE-347 (Improper Verification of Cryptographic Signature) and CWE-287 (Improper Authentication), indicating the Cloud Authentication Service fails to properly validate identity assertions. Relevant MITRE ATT&CK techniques include T1190 (Exploit Public-Facing Application), T1133 (External

Remote Services), T1078 (Valid Accounts, authentication bypass producing valid session), and T1556 (Modify Authentication Process). As of the May 13, 2026 disclosure, hotfixes were partially pending across all four branches. No active exploitation in the wild has been observed. Palo Alto Networks rates urgency as HIGHEST. Cloud NGFW and Prisma Access are confirmed not affected. Refer to the NVD entry (https://nvd.nist.gov/vuln/detail/CVE-2026-0265) and the Palo Alto Networks security advisory for vendor-confirmed patch status and mitigation guidance.

Action Checklist

1. Step 1: Containment. Identify all PA-Series firewalls, VM-Series firewalls, and Panorama appliances running PAN-OS 10.2, 11.1, 11.2, or 12.1. Disable the Cloud Authentication Service on any management interface that is network-reachable from untrusted segments. If disabling the service is not operationally feasible, restrict management interface access to a dedicated out-of-band management network with strict ACLs. Consult the Palo Alto Networks security advisory for vendor-confirmed mitigation steps specific to your PAN-OS branch.
2. Step 2: Detection. Query firewall and Panorama management plane logs for unexpected authentication events, session establishments without corresponding credential prompts, or anomalous API calls originating from untrusted source IPs. Review PAN-OS system logs (monitor > logs > system) for authentication-related events tied to Cloud Authentication Service. Look for behavioral indicators consistent with T1190 and T1078: successful management plane sessions from external IPs with no prior authentication challenge recorded. No public IOCs have been reported as of disclosure; focus detection on access pattern anomalies rather than signature-based IOC matching.
3. Step 3: Eradication. Apply all available hotfixes for your affected PAN-OS branch (10.2.x, 11.1.x, 11.2.x, or 12.1.x) per the Palo Alto Networks advisory. For branches where hotfixes remain pending, maintain the Cloud Authentication Service disabled or management interface isolated until a patch is confirmed available. Do not re-enable the Cloud Authentication Service on network-reachable interfaces until the patch is applied and verified. Confirm patch availability directly from the advisory; patch status varies by branch.
4. Step 4: Recovery. After patching, re-enable the Cloud Authentication Service only on intended interfaces and verify authentication flows function correctly. Review management plane access logs for any unauthorized sessions that may have occurred in the exposure window between the Cloud Authentication Service being enabled and the patch being applied. Rotate any credentials or session tokens that may have been accessible via the management interface. Confirm no unauthorized accounts were created or configuration changes were made.
5. Step 5: Post-Incident. Audit management interface exposure across all firewall and Panorama deployments; management interfaces should never be reachable from untrusted networks. Review whether Cloud Authentication Service configurations follow the principle of least exposure. Evaluate network segmentation controls between management planes and production traffic paths. Map this incident to NIST CSF PR.AC (Identity Management and Access Control) and PR.PT (Protective Technology) control gaps. Update vulnerability management SLAs to prioritize CVSS High/Critical findings on network security devices to under 72 hours for containment action.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance if Monitor > Logs > Configuration shows any unauthorized admin account creation, policy changes, or configuration exports during the exposure window, or if any affected PAN-OS device processes traffic subject to PCI-DSS, HIPAA, or state breach notification requirements — exploitation of this bypass grants unauthenticated full management plane control, meaning any such activity constitutes a confirmed breach of a network security control plane.
Recovery Notes	After applying CVE-2026-0265 hotfixes, monitor PAN-OS system logs (Monitor > Logs > System, subtype: auth) continuously for a minimum of 30 days post-recovery for any recurrence of authentication anomalies, paying particular attention to successful management plane sessions from unexpected source IPs. Validate that the Cloud Authentication Service is functioning correctly by performing authenticated test logins from approved administrator workstations and confirming that authentication challenge events appear in the system log for every session — absence of a challenge record for a successful session remains the key behavioral indicator of re-exploitation. Retain all forensic artifacts (configuration snapshots, log exports, diff outputs) for a minimum of 12 months or per your incident retention policy, as the management plane access granted by this bypass could have been used to establish persistence mechanisms that surface only after recovery.
Forensic Artifacts	PAN-OS System Log (Monitor > Logs > System, subtype: auth) for the full exposure window: the primary exploit indicator is a 'login succeeded' or session-creation event with no preceding authentication challenge from the same source IP, which is the behavioral signature of the CVE-2026-0265 bypass of the Cloud Authentication Service credential validation flow | PAN-OS Configuration Audit Log (Monitor > Logs > Configuration): captures every configuration change made through the management plane including admin account creation, policy modifications, and configuration exports — any changes originating from an unrecognized source IP or outside of approved change windows during the exposure window indicate post-exploitation adversary activity | PAN-OS running configuration diff (pre-patch 'show config running' export vs. known-good baseline): identifies persistence mechanisms such as backdoor admin accounts, modified admin role profiles, rogue API keys, or altered security policy rules that an attacker with unauthenticated management plane access could have introduced | PAN-OS session table and traffic logs for management plane source IPs: 'show session all filter application ssl' filtered to management interface destination IPs, cross-referenced with netflow or interface counters, to identify data exfiltration of the device configuration or use of the compromised management plane as a pivot point into adjacent network segments | API key and administrator credential audit output ('show admins all', 'show admin-profile all', 'request api-key list' if available): documents the complete set of API keys and administrator accounts active during the exposure window, enabling identification of any credentials generated or leveraged by an attacker exploiting the authentication bypass to authenticate subsequent management sessions without triggering further alerts

Per-Action IR Details

Step 1: Containment — Identify all PA-Series firewalls, VM-Series firewalls, and Panorama appliances running PAN-OS 10.2, 11.1, 11.2, or 12.1. Disable the Cloud Authentication Service on any management interface that is network-reachable from untrusted segments. If disabling the service is not operationally feasible, restrict management interface access to a dedicated out-of-band management network with strict ACLs. Reference the Palo Alto Networks security advisory at https://security.paloaltonetworks.com/CVE-2026-0265 for vendor-confirmed mitigation steps (verify the advisory reflects the most current guidance).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems to prevent further exploitation while maintaining operational continuity where possible

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run 'show system info' and 'show devices all' via PAN-OS CLI or Panorama to enumerate all managed devices and their PAN-OS versions; export results to CSV. Use a simple bash or PowerShell script to compare version strings against affected branches (10.2, 11.1, 11.2, 12.1). To confirm Cloud Authentication Service status, run 'show authentication setting' from the PAN-OS CLI on each device. Block TCP/443 and TCP/22 to management interfaces from untrusted subnets using upstream ACLs on any intervening switch or router if a dedicated OOB management VLAN cannot be immediately provisioned.

Evidence: Before disabling Cloud Authentication Service or modifying ACLs, capture: (1) PAN-OS 'show system state' output to record current management interface bindings and active sessions; (2) 'show admins all' CLI output to document all currently logged-in administrator sessions on the management plane; (3) full running configuration snapshot via 'show config running' exported and hashed (SHA-256) for integrity baseline; (4) PAN-OS system log export (Monitor > Logs > System) filtered to the prior 30 days for auth-category events, preserving pre-containment state; (5) network flow or firewall session table ('show session all') to capture any active management plane sessions from external IPs prior to ACL enforcement.

Step 2: Detection — Query firewall and Panorama management plane logs for unexpected authentication events, session establishments without corresponding credential prompts, or anomalous API calls originating from untrusted source IPs. Review PAN-OS system logs (monitor > logs > system) for authentication-related events tied to Cloud Authentication Service. Look for behavioral indicators consistent with T1190 and T1078: successful management plane sessions from external IPs with no prior authentication challenge recorded. No public IOCs have been reported as of disclosure; focus detection on access pattern anomalies rather than signature-based IOC matching.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate management plane log sources to identify bypass indicators; authentication bypass exploits leave session establishment records without corresponding credential exchange artifacts

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Export PAN-OS system logs via syslog to a local rsyslog or syslog-ng instance (free). Parse exported logs with grep or awk: 'grep -i "auth\|login\|session\|cloud-auth" /var/log/panos_system.log | grep -v "failed"' to surface successful authentications lacking a preceding credential prompt entry. For API call auditing, query the PAN-OS Management Plane log (Monitor > Logs > System, subtype: auth) for entries where the source IP falls outside your known administrator IP allowlist. Write a Sigma rule targeting PAN-OS syslog events with facility 'authpriv' and outcome 'success' where source IP is not in a defined safe-list — Sigma can be converted to grep patterns for teams without a SIEM. Cross-reference any flagged source IPs against Shodan or RIPE WHOIS manually for geolocation/ASN anomalies.

Evidence: Query PAN-OS system log (Monitor > Logs > System) filtering on 'subtype eq auth' for the full exposure window (date Cloud Authentication Service was enabled through current date); flag any 'login succeeded' or session-creation events where no preceding 'authentication requested' entry appears from the same source IP within the same session context — this absence-of-challenge pattern is the primary behavioral indicator of CVE-2026-0265 exploitation. Additionally query the PAN-OS configuration audit log (Monitor > Logs > Configuration) for any changes made during suspected bypass sessions, which would indicate post-authentication adversary activity consistent with MITRE T1078 (Valid Accounts) and T1190 (Exploit Public-Facing Application). Capture Panorama management plane access logs if Panorama is present, as a compromised Panorama instance would have downstream reach to all managed devices.

Step 3: Eradication — Apply all available hotfixes for your affected PAN-OS branch (10.2.x, 11.1.x, 11.2.x, or 12.1.x) per the Palo Alto Networks advisory. For branches where hotfixes remain pending, maintain the Cloud Authentication Service disabled or management interface isolated until a patch is confirmed available. Do not re-enable the Cloud Authentication Service on network-reachable interfaces until the patch is applied and verified. Confirm patch availability directly from the advisory; patch status was partially pending at time of disclosure on May 13, 2026.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the vulnerability from the environment by applying vendor-issued hotfixes for CVE-2026-0265 and confirming Cloud Authentication Service is disabled on all management interfaces pending patch availability per branch

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-7 (Least Functionality), NIST IR-4 (Incident Handling), 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: For teams without automated patch management: download PAN-OS hotfixes directly from the Palo Alto Networks support portal (support.paloaltonetworks.com) and validate the downloaded image SHA-256 hash against the portal-published checksum before installation — do not skip hash verification. Stage hotfix installation during a maintenance window; use 'request system software install' CLI command and follow with 'show system info' post-reboot to confirm the new version string reflects the patched build. For pending-patch branches, document the compensating control (service disabled or OOB isolation) formally in your risk register with a review date tied to Palo Alto's advisory update cadence.

Evidence: Before applying any hotfix, preserve a forensic snapshot of the potentially compromised management plane: export the full configuration ('export configuration' via CLI or GUI), capture 'show system state filter-pretty' output, and export all system and configuration audit logs covering the exposure window. Hash all captured files (SHA-256) and store offline. After patching, run 'show system info' to confirm the installed version matches the CVE-2026-0265 hotfix build number published in the Palo Alto advisory — retain this output as eradication verification evidence. If compromise is suspected, these pre-patch artifacts are your forensic baseline before any remediation changes alter the system state.

Step 4: Recovery — After patching, re-enable the Cloud Authentication Service only on intended interfaces and verify authentication flows function correctly. Review management plane access logs for any unauthorized sessions that may have occurred in the exposure window between the Cloud Authentication Service being enabled and the patch being applied. Rotate any credentials or session tokens that may have been accessible via the management interface. Confirm no unauthorized accounts were created or configuration changes were made.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore services with verified integrity, validate that authentication flows through Cloud Authentication Service are functioning as expected post-patch, and confirm no adversary persistence mechanisms were introduced during the exposure window

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Run 'show admins all' and 'show admin-profile all' on each affected PAN-OS device to enumerate all administrator accounts; compare against your known-good account inventory (CIS 5.1) and flag any accounts not in the baseline. Review 'show config running | match admin' output to identify any admin accounts added during the exposure window. For credential rotation without an enterprise PAM tool: use the PAN-OS GUI or CLI to reset all local administrator passwords, revoke and reissue any API keys ('request api-key generate'), and if LDAP/RADIUS integration is in use, coordinate with the directory team to force session invalidation for accounts with management plane access. Document all rotation actions with timestamps.

Evidence: Audit the PAN-OS configuration log (Monitor > Logs > Configuration) for the full exposure window to identify any configuration changes — pay specific attention to new administrator account creation, changes to admin roles or profiles, firewall policy modifications, or NAT rule additions that could indicate adversary persistence or lateral movement staging. Cross-reference the 'show config running' snapshot taken at containment against the current running config using a diff tool to surface any delta introduced during the exposure window. Review PAN-OS system log entries for 'admin' and 'config' subtypes to reconstruct the complete timeline of management plane activity between Cloud Authentication Service enablement and patch application.

Step 5: Post-Incident — Audit management interface exposure across all firewall and Panorama deployments; management interfaces should never be reachable from untrusted networks. Review whether Cloud Authentication Service configurations follow the principle of least exposure. Evaluate network segmentation controls between management planes and production traffic paths. Map this incident to NIST CSF PR.AC (Identity Management and Access Control) and PR.PT (Protective Technology) control gaps. Update vulnerability management SLAs to prioritize CVSS High/Critical findings on network security devices to under 72 hours for containment action.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review to identify why PAN-OS management interfaces were reachable from untrusted segments, update detection capabilities for future Cloud Authentication Service exposure, and refine vulnerability SLAs for network security infrastructure

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST CA-7 (Continuous Monitoring), NIST SC-7 (Boundary Protection), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Perform a management interface exposure audit using nmap from an untrusted VLAN perspective: 'nmap -p 443,22,3978 --open ' to confirm management plane ports are not reachable from production or external segments — document and remediate any reachable hosts. Subscribe to Palo Alto Networks Security Advisories RSS feed (no cost) and configure a free RSS-to-email gateway or use a Slack webhook integration so future advisories arrive within hours of publication. Update your vulnerability management SLA policy document to classify CVSS ≥7.0 findings on network security devices (firewalls, Panorama, VPN concentrators) as requiring containment action within 72 hours, and track SLA compliance in a simple spreadsheet if no GRC tool is available.

Evidence: Produce a lessons-learned report documenting: (1) which PAN-OS versions and how many devices were exposed and for how long (exposure window duration per device); (2) whether any detection gaps prevented earlier identification of the advisory — specifically, whether SI-5 (Security Alerts) processes would have surfaced the Palo Alto advisory within 24 hours of publication; (3) results of the management interface exposure audit showing which interfaces were reachable from untrusted networks and the remediation status. Retain all forensic artifacts from steps 1-4 per your audit record retention policy (NIST AU-11) and document the incident in your incident tracking system (NIST IR-5) with a full timeline from advisory publication through verified eradication.

Detection Guidance

No public IOCs (IPs, domains, hashes) have been reported as of the May 13, 2026 disclosure. Detection should focus on behavioral and log-based indicators. In PAN-OS system logs (Monitor > Logs > System), filter for authentication events associated with the Cloud Authentication Service, particularly successful management plane authentications that lack a corresponding credential challenge entry. Review management plane access logs for sessions originating from unexpected external or untrusted source IPs. In Panorama, correlate device management access events across managed firewalls for anomalous access patterns. Relevant MITRE techniques to hunt for: T1190 (management interface exploitation attempts, look for HTTP/HTTPS requests to management plane URLs from non-management source IPs), T1078 (valid session tokens appearing without prior authentication sequence), T1556 (unexpected changes to authentication configuration). If a SIEM ingests

PAN-OS syslog, write detection logic for authentication events where the source IP is outside the approved management network range and the authentication result is 'success'. Given no in-the-wild exploitation is confirmed, priority should be on verifying exposure (Cloud Authentication Service enabled + reachable interface) rather than active compromise hunting, unless logs show suspicious access during the exposure window.

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1078** — Valid Accounts
- **T1556** — Modify Authentication Process
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SC-13** — Cryptographic Protection
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

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

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography
- **A.5.23** — Information security for use of cloud services

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
T1133	External Remote Services	Persistence
T1078	Valid Accounts	Defense-Evasion
T1556	Modify Authentication Process	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Palo Alto Networks Security Advisories	https://security.paloaltonetworks.com/CVE-2026-0265	T3
	https://www.flyingpenguin.com/	T3
CVE-2026-0265 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-0265	T1
CVE-2026-26265: Discourse IDOR Information Disclosure Flaw	https://www.sentinelone.com/vulnerability-database/cve-2026-26265/	T3
CVE-2026-27265 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-27265	T1

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