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

PAN-OS IKEv2 Buffer Overflow Enables Unauthenticated RCE on PQC-Enabled Firewalls (CVE-2026-0263)

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0168
Type	CVE Vulnerability
CVE ID	CVE-2026-0263
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Palo Alto Networks PAN-OS 11.1 (multiple hotfix branches), PAN-OS 11.2 (multiple hotfix branches), PAN-OS 12.1 (multiple hotfix branches). NOT affected: PAN-OS 10.2, Cloud NGFW, Prisma Access.
Published	2026-05-13T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

A high-severity unauthenticated remote code execution vulnerability in Palo Alto Networks PAN-OS affects firewalls running IKEv2 VPN tunnels with Post-Quantum Cryptography ciphers enabled, across PAN-OS versions 11.1, 11.2, and 12.1. A successful exploit gives an attacker full control of the perimeter firewall without any credentials, potentially exposing the entire network it protects. Organizations with affected configurations should treat this as operationally critical and apply patches or mitigations immediately.

Technical Analysis

CVE-2026-0263 is a heap and stack buffer overflow (CWE-787, CWE-121) in the IKEv2 processing component of PAN-OS. An unauthenticated remote attacker sends malformed IKEv2 packets to a targeted firewall, triggering arbitrary code execution at elevated privileges or a denial-of-service condition. Exploitation is conditional: the firewall must have Post-Quantum Cryptography (PQC) ciphers configured on IKEv2 VPN tunnels. Affected versions: PAN-OS 11.1 (multiple hotfix branches), 11.2 (multiple hotfix branches), 12.1 (multiple hotfix branches). Not affected: PAN-OS 10.2, Cloud NGFW, Prisma Access. CVSS base score is 7.5 (high severity); however, the unauthenticated, network-facing, RCE-capable attack surface on perimeter infrastructure warrants critical operational treatment. MITRE techniques: T1190 (Exploit Public-Facing

Application), T1068 (Exploitation for Privilege Escalation), T1499 (Endpoint Denial of Service). No confirmed active exploitation at time of vendor disclosure. No CISA KEV listing at time of disclosure. Primary advisory: Palo Alto Networks PSIRT (https://security.paloaltonetworks.com/CVE-2026-0263). NVD record: https://nvd.nist.gov/vuln/detail/CVE-2026-0263.

Action Checklist

1. Step 1: Containment. Identify all PAN-OS firewalls running versions 11.1, 11.2, or 12.1 with IKEv2 VPN configured. If PQC ciphers are enabled on any IKEv2 tunnel, disable PQC cipher configuration immediately as a temporary mitigation until patching is complete. Restrict IKEv2 traffic to trusted peer IPs at the perimeter where operationally feasible. Source: Palo Alto Networks PSIRT advisory (https://security.paloaltonetworks.com/CVE-2026-0263).
2. Step 2: Detection. Query firewall management logs and IKEv2/IKE daemon logs for malformed or anomalous IKEv2 packet sequences, unexpected daemon crashes or restarts, and privilege escalation events on PAN-OS management plane. Review threat logs for repeated IKEv2 negotiation failures from external IPs. Check system logs for core dumps or unexpected process exits in the IKE subsystem. Consult the Palo Alto Networks PSIRT advisory for any vendor-published indicators specific to this CVE.
3. Step 3: Eradication. Apply the vendor-released hotfix for your affected PAN-OS branch (11.1, 11.2, or 12.1) as published in the Palo Alto Networks PSIRT advisory. If a hotfix for your specific branch is not yet available, maintain PQC cipher disablement on IKEv2 tunnels as a temporary workaround until the patch is released and applied. Confirm patch version numbers against the advisory before deployment.
4. Step 4: Recovery. After patching, re-enable PQC ciphers only if required and confirm IKEv2 tunnel stability. Validate firewall policy integrity and review management plane configurations for unauthorized changes. Monitor IKEv2 and system logs for residual anomalous activity for at least 72 hours post-patch. Confirm the patched version appears correctly in PAN-OS system info output.
5. Step 5: Post-Incident. Evaluate whether PQC cipher adoption outpaced compensating control readiness on perimeter devices. Review the process for tracking vendor urgency that may diverge from CVSS scores. Assess whether IKEv2 endpoints are segmented from management interfaces. Document this event as a case study for cryptographic modernization risk management.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and initiate formal incident declaration if: (1) any ikemgr or iked core dump is found in /var/cores/ predating the advisory, indicating likely exploitation prior to containment; (2) post-exploitation artifacts are found (unauthorized admin accounts, new API keys, modified security policies, or unexpected outbound connections from the firewall management plane); or (3) the affected PAN-OS firewall protects environments in scope for PCI DSS, HIPAA, or other breach-notification frameworks, as unauthenticated RCE on a perimeter firewall constitutes a presumptive breach requiring legal and compliance review.

Recovery Notes	After applying the vendor hotfix for the affected PAN-OS branch (11.1, 11.2, or 12.1), verify the exact version string via 'show system info' against the PSIRT advisory before re-enabling PQC ciphers on any IKEv2 profile. Perform a full configuration diff between the pre-incident baseline export and the post-patch running config, paying specific attention to administrator accounts, API keys, and IKE gateway definitions for unauthorized modifications that could indicate pre-patch exploitation. Maintain elevated monitoring of PAN-OS system logs for ikemgr restart events and anomalous IKEv2 negotiation patterns for a minimum of 72 hours post-patch, extending to 7 days if any exploitation indicators were identified during detection.
Forensic Artifacts	/var/cores/ directory on affected PAN-OS devices — core dump files from ikemgr or iked processes are the highest-confidence forensic indicator of successful buffer overflow exploitation of CVE-2026-0263; preserve with timestamps before any reboot or patch cycle | PAN-OS system log (/var/log/pan/system.log) filtered for 'ikemgr', 'iked', 'unexpected restart', 'process exited', and 'segfault' — these entries record IKE daemon crashes that a CVE-2026-0263 exploit attempt would trigger during buffer overflow execution | PAN-OS traffic logs for UDP 500 and UDP 4500 — high-volume IKE_SA_INIT requests from a single external IP, especially those followed by an ikemgr crash, indicate exploit iteration against the PQC cipher extension processing code path; correlate source IPs across traffic and threat logs | IKEv2 session table snapshot from 'show vpn ike-sa detail' — captures peer IP addresses, negotiated cipher suites, and session age at time of discovery; sessions negotiated with PQC algorithms from unrecognized peer IPs are high-priority forensic leads | Pre- and post-incident running configuration exports ('show config running' in XML) — diff these files to identify unauthorized changes to admin accounts, API key entries, IKE crypto profiles, or security policies that would indicate successful post-exploitation activity on the PAN-OS management plane

Per-Action IR Details

Step 1: Containment — Identify all PAN-OS firewalls running versions 11.1, 11.2, or 12.1 with IKEv2 VPN configured. If PQC ciphers are enabled on any IKEv2 tunnel, disable PQC cipher configuration immediately as a temporary mitigation until patching is complete. Restrict IKEv2 traffic to trusted peer IPs at the perimeter where operationally feasible. Source: Palo Alto Networks PSIRT advisory (https://security.paloaltonetworks.com/CVE-2026-0263).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems and implement short-term containment to limit damage while preserving evidence

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality) — disable PQC cipher profiles on IKEv2 crypto maps to remove the vulnerable code path, NIST SC-8 (Transmission Confidentiality and Integrity) — enforcing trusted-peer IP restrictions on UDP 500/4500 limits the unauthenticated attack surface, CIS 4.4 (Implement and Manage a Firewall on Servers) — apply perimeter ACLs restricting IKEv2 UDP 500/4500 to known VPN peer addresses, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — inventory all PAN-OS 11.1/11.2/12.1 devices with active IKEv2 profiles before any cipher change

Compensating: Run 'show vpn ike-sa' and 'show vpn flow' from PAN-OS CLI on each firewall to enumerate active IKEv2 tunnels and identify PQC cipher profiles. To identify PQC-enabled crypto profiles, run: 'show running security-policy | match pqc' or navigate Panorama > Network > IKE Crypto Profiles and filter for post-quantum algorithm entries. For perimeter restriction without a next-gen ACL platform, use the PAN-OS security policy to create a pre-rulebase deny for IKEv2 (UDP 500, UDP 4500) with a source zone of 'untrust' and destination negation of your known peer IP list — export the peer list first via 'show vpn gateway' to avoid disrupting legitimate tunnels.

Evidence: Before disabling PQC ciphers, capture: (1) full 'show vpn ike-sa detail' output for all active IKEv2 sessions — this preserves peer IP addresses, cipher negotiation state, and session age that may indicate an already-exploited session; (2) PAN-OS system log snapshot from /var/log/pan/system.log filtered for 'ikemgr' or 'iked' entries in the 24–72

hours preceding discovery; (3) a running configuration export ('show config running') to document the exact PQC cipher profile names and IKEv2 gateway assignments prior to any change, creating a forensic baseline. Preserve these before any configuration modification.

Step 2: Detection — Query firewall management logs and IKEv2/IKE daemon logs for malformed or anomalous IKEv2 packet sequences, unexpected daemon crashes or restarts, and privilege escalation events on PAN-OS management plane. Review threat logs for repeated IKEv2 negotiation failures from external IPs. Check system logs for core dumps or unexpected process exits in the IKE subsystem. Consult the Palo Alto Networks PSIRT advisory for any vendor-published indicators specific to this CVE.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate log sources, identify precursor and indicator patterns, and determine scope of compromise

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring) — track ikemgr crash events and IKEv2 negotiation failures as incident indicators across all affected PAN-OS versions, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — structured review of PAN-OS system and threat logs for IKE daemon anomalies, NIST AU-12 (Audit Record Generation) — confirm IKEv2 daemon logging and core dump capture are enabled on all 11.1/11.2/12.1 instances, NIST SI-4 (System Monitoring) — monitor management plane process table for unexpected ikemgr or iked spawns indicating post-exploit persistence, CIS 8.2 (Collect Audit Logs) — ensure PAN-OS syslog forwarding is active for system, threat, and traffic log categories before analysis begins

Compensating: Without a SIEM, use Panorama log forwarding to a syslog server and run grep queries directly: 'grep -i "ikemgr\|iked\|core\|segfault\|buffer overflow" /var/log/pan/system.log' on each firewall over SSH. For crash evidence, check 'ls -lt /var/cores/' — any .core file timestamped within your window of concern is high-priority evidence. Query PAN-OS threat logs via CLI: 'show log threat direction equal server threat-name contains "IKE"' to surface repeated IKEv2 negotiation failures from single source IPs. Use Wireshark on a mirror/TAP port for UDP 500/4500 to capture IKEv2 INIT and AUTH exchanges; malformed CVE-2026-0263 payloads targeting the PQC extension fields should appear as oversized or malformed SA payload attributes in the IKE_SA_INIT message.

Evidence: Collect before any system restart or patch: (1) /var/cores/ directory — core dump files from ikemgr or iked processes are the highest-confidence indicator of successful buffer overflow exploitation of this CVE; (2) PAN-OS system log entries (Panorama > Monitor > Logs > System, or /var/log/pan/system.log) filtered for severity 'critical' or 'high' with description matching 'ikemgr', 'iked', 'unexpected restart', or 'process exited'; (3) PAN-OS traffic logs for UDP 500/4500 showing high-volume IKE_SA_INIT requests from a single external IP, which would indicate pre-exploit reconnaissance or exploit iteration; (4) PAN-OS threat log entries for 'IKEv2' negotiation failures correlated with the same source IPs appearing in traffic logs — pattern of failure followed by success is an exploitation indicator.

Step 3: Eradication — Apply the vendor-released hotfix for your affected PAN-OS branch (11.1, 11.2, or 12.1) as published in the Palo Alto Networks PSIRT advisory. If a hotfix for your specific branch is not yet available, maintain PQC cipher disablement on IKEv2 tunnels as a temporary workaround until the patch is released and applied. Confirm patch version numbers against the advisory before deployment.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: eliminate the root cause of the incident, including removing malicious code and applying vendor fixes

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation) — apply the Palo Alto Networks PSIRT-designated hotfix for PAN-OS 11.1, 11.2, or 12.1 to remediate the IKEv2 buffer overflow in the PQC cipher processing code path, NIST SI-7 (Software, Firmware, and Information Integrity) — verify the downloaded PAN-OS hotfix image SHA256 hash against the value published in the PSIRT advisory before installation, NIST CM-3 (Configuration Change Control) — document the exact pre- and post-patch PAN-OS version via 'show system info' output as change management evidence, CIS 7.3 (Perform Automated Operating System Patch Management) — prioritize PAN-OS 11.1/11.2/12.1 hotfix deployment within vendor-recommended urgency window, CIS 7.4 (Perform Automated Application Patch Management) — treat PAN-OS hotfix as an application-layer patch requiring staged rollout with rollback plan

Compensating: Before applying the hotfix, export the full device configuration: 'scp export configuration from running-config.xml to ' — this serves as both a rollback artifact and a forensic baseline. Verify the downloaded hotfix image integrity by running 'show system software status' post-install and cross-referencing the reported version string against the exact version number in the PSIRT advisory (e.g., PAN-OS 11.2.x-hx). If the hotfix requires a reboot, schedule during a maintenance window and pre-stage on Panorama using the 'Device > Software' workflow to minimize manual error. For branch-specific hotfix availability gaps, document the PQC cipher disablement state in your change management system with a review trigger tied to the PSIRT advisory update feed.

Evidence: Capture before patching: (1) 'show system info' output — records the exact pre-patch PAN-OS version string (e.g., 11.2.3-h2) for the change record and confirms you are patching the correct branch; (2) 'show running-config' export — preserves the IKEv2 and IKE crypto profile configuration state so post-patch comparison can identify any configuration drift introduced during eradication; (3) if exploitation is suspected, collect /var/cores/ and /var/log/pan/system.log before the patch reboot, as a reboot will rotate logs and may purge core files depending on PAN-OS storage management settings.

Step 4: Recovery — After patching, re-enable PQC ciphers only if required and confirm IKEv2 tunnel stability. Validate firewall policy integrity and review management plane configurations for unauthorized changes. Monitor IKEv2 and system logs for residual anomalous activity for at least 72 hours post-patch. Confirm the patched version appears correctly in PAN-OS system info output.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to normal operations, verify system integrity, and confirm threat has been eliminated before returning to production

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification) — verify IKEv2 tunnel re-establishment and PQC cipher negotiation behaves correctly post-patch before re-enabling in production, NIST SI-7 (Software, Firmware, and Information Integrity) — diff the running configuration against the pre-patch baseline export to identify any unauthorized changes introduced during a potential exploitation window, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — conduct structured 72-hour post-patch log review of PAN-OS system and IKEv2 daemon logs for residual indicators, NIST CM-3 (Configuration Change Control) — document re-enablement of PQC ciphers as a discrete change event with business justification and approval, CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure) — compare post-patch firewall configuration against the documented secure baseline before returning to full production

Compensating: Run 'show system info' immediately post-reboot and confirm the version string matches the PSIRT-designated hotfix exactly — screenshot or log capture this output as your patch verification record. To check for unauthorized management plane changes, diff the pre-patch and post-patch running configs: export both and run 'diff pre-patch-config.xml post-patch-config.xml' — look specifically for changes to admin accounts, API key entries, security policies, and IKE gateway definitions. For 72-hour monitoring without a SIEM, schedule a twice-daily manual review of 'show log system' filtered for 'ikemgr' and 'iked' entries, and set PAN-OS email alerts for process restart events via Device > Server Profiles > Email.

Evidence: Post-patch, preserve: (1) 'show system info' output confirming the exact hotfix version — this is your primary patch verification artifact; (2) output of 'show vpn ike-sa' and 'show vpn flow' after tunnel re-establishment — confirms IKEv2 sessions are re-negotiating with expected parameters and no ghost sessions from a pre-exploitation window persist; (3) PAN-OS system log entries for the 72-hour post-patch window, specifically filtered for ikemgr restart events — any recurrence after patching would indicate a separate unpatched instance or a persistence mechanism introduced via pre-patch exploitation.

Step 5: Post-Incident — Evaluate whether PQC cipher adoption outpaced compensating control readiness on perimeter devices. Review the process for tracking vendor urgency ratings that diverge from CVSS scores. Assess whether IKEv2 endpoints are segmented from management interfaces. Document this event as a case study for cryptographic modernization risk management.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review, update IR plan and detection capabilities, and share intelligence to prevent recurrence

Controls: NIST IR-4 (Incident Handling) — update the IR playbook to include PAN-OS IKEv2 daemon crash as a monitored indicator and add PQC cipher status to the perimeter device hardening checklist, NIST IR-8 (Incident Response Plan) — revise the plan to incorporate a vendor urgency rating ingestion process that flags PSIRT advisories rated 'HIGHEST' regardless of CVSS base score, NIST RA-3 (Risk Assessment) — document the risk introduced by deploying PQC ciphers on perimeter devices ahead of compensating control maturity as a formal risk register entry, NIST SC-32 (System Partitioning) — assess and document whether PAN-OS management interfaces (web UI, SSH, Panorama) are on a separate management VLAN isolated from IKEv2 VPN gateway interfaces, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — update the vulnerability management SOP to include a PSIRT advisory review step that correlates vendor urgency ratings against internal asset criticality, not CVSS alone, CIS 7.2 (Establish and Maintain a Remediation Process) — establish a documented SLA for perimeter firewall patches rated 'HIGHEST urgency' by Palo Alto Networks PSIRT that is shorter than the standard monthly patching cycle

Compensating: For the management plane segmentation assessment, run 'show interface management' and 'show system setting management-interface' on each affected PAN-OS device to confirm the management interface is bound to a dedicated out-of-band VLAN and not reachable from the IKEv2 VPN zone. Document findings in a one-page architecture review. For the PSIRT monitoring gap, create a free PSIRT RSS feed subscription (https://security.paloaltonetworks.com/rss.xml — note: verify this URL resolves before use) and route it to a shared team inbox with a filter rule flagging any advisory rated 'CRITICAL' or 'HIGHEST urgency' for same-day review. This is achievable with no-cost email tooling.

Evidence: For the lessons-learned record, assemble: (1) timeline of when the PSIRT advisory was published versus when your team became aware — this gap is the primary metric for improving your threat intel ingestion process; (2) inventory export showing all PAN-OS 11.1/11.2/12.1 devices with IKEv2 and PQC cipher configuration, which quantifies the blast radius and informs future architecture decisions around PQC rollout sequencing; (3) the pre- and post-patch configuration diffs from Step 4 — these serve as the case study evidence for cryptographic modernization risk management and should be retained per your incident record retention policy under NIST AU-11 (Audit Record Retention).

Detection Guidance

Focus detection on the IKEv2 processing layer. In PAN-OS system logs, look for IKE daemon crashes, unexpected restarts, or core dump events. In traffic logs, flag repeated IKEv2 negotiation failures or malformed packet errors from external source IPs, particularly those targeting UDP port 500 or 4500. Look for privilege escalation events or unexpected process spawning on the management plane following IKEv2 activity. If your SIEM ingests PAN-OS syslog, create an alert for IKE daemon fault or IKE process exit within a short time window of external IKEv2 connection attempts. No public IOCs or exploit signatures have been confirmed at time of disclosure; update detection rules as the Palo Alto Networks PSIRT advisory is revised.

Framework Mappings

MITRE-ATTACK

- **T1068** — Exploitation for Privilege Escalation
- **T1190** — Exploit Public-Facing Application
- **T1499** — Endpoint Denial of Service

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **SC-5** — Denial-of-Service Protection
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation
- **SR-2** — Supply Chain Risk Management Plan
- **SC-13** — Cryptographic Protection
- **IR-5** — Incident Monitoring

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **15.1** — Establish and Maintain an Inventory of Service Providers

OWASP-TOP10-2021

- **A03:2021** — Injection

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1190	Exploit Public-Facing Application	Initial-Access
T1499	Endpoint Denial of Service	Impact

Sources

Source	URL	Tier
Palo Alto Networks Security Advisories	https://security.paloaltonetworks.com/CVE-2026-0263	T3
CVE-2026-26263 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-26263	T3
CVE-2026-26263 Security Vulnerability Analysis & Exploit Details	https://cve.akaoma.com/cve-2026-26263	T3
ZDI-26-263 - Zero Day Initiative	https://www.zerodayinitiative.com/advisories/ZDI-26-263/	T3
RHSA-2026:0263 - Security Advisory - Red Hat Customer Portal	https://access.redhat.com/errata/RHSA-2026:0263	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-0263	T1

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