INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-13 14:28 UTC

PAN-OS DNS Proxy Buffer Overflow Opens PA-Series Firewalls to Unauthenticated RCE, Patches Partially Available

CVE VULNERABILITY | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0167
Type	CVE Vulnerability
CVE ID	CVE-2026-0264
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Palo Alto Networks PAN-OS versions 10.2, 11.1, 11.2, and 12.1 on PA-Series hardware and VM-Series firewalls; Panorama, Cloud NGFW, and Prisma Access are not affected
Published	2026-05-13T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

Palo Alto Networks disclosed a heap-based buffer overflow in PAN-OS (CVE-2026-0264) on May 13, 2026, affecting PA-Series hardware and VM-Series firewalls running versions 10.2, 11.1, 11.2, and 12.1. An unauthenticated remote attacker can exploit the DNS Proxy component to execute arbitrary code directly on the firewall, potentially gaining full control of network perimeter defenses. Patches are not yet available for all affected versions as of the disclosure date; check the Palo Alto Networks PSIRT advisory for current patch availability and timeline.

Technical Analysis

CVE-2026-0264 is a heap-based buffer overflow (CWE-122; also classified under CWE-119 improper restriction of operations within memory bounds) in the DNS Proxy and DNS Server components of PAN-OS. Affected versions: 10.2, 11.1, 11.2, and 12.1 on PA-Series hardware firewalls and VM-Series firewalls. Panorama, Cloud NGFW, and Prisma Access are explicitly not affected per vendor advisory. The vulnerability allows an unauthenticated remote attacker to send malformed DNS requests to the DNS Proxy listener, triggering a heap overflow that can result in arbitrary code execution at the firewall process level. MITRE techniques mapped include T1190 (Exploit Public-Facing Application), T1203 (Exploitation for Client Execution), T1059 (Command and Scripting Interpreter), T1133 (External Remote Services), and T1499 (Endpoint Denial of Service). CVSS base score reported as 7.5. Palo Alto Networks rates urgency as HIGHEST. Patches are partially available; not

all affected release branches have fixes published as of the disclosure date. Primary authoritative source: Palo Alto Networks PSIRT advisory.

Action Checklist

1. Step 1: Containment, Identify all PA-Series hardware and VM-Series firewalls running PAN-OS 10.2, 11.1, 11.2, or 12.1. Immediately disable DNS Proxy on any interface directly reachable from the internet if DNS Proxy is not operationally required. Restrict DNS Proxy access to trusted internal segments via security policy until patches are applied. Reference: Palo Alto Networks PSIRT advisory for CVE-2026-0264 for interface-specific mitigation guidance.
2. Step 2: Detection, Query firewall management logs and system logs for unexpected process crashes or restarts in the DNS Proxy service (dnsproxyd). Review traffic logs for high-volume or malformed DNS request patterns directed at PA-Series management or data-plane interfaces with DNS Proxy enabled. Check for anomalous outbound connections from firewall processes post-DNS activity, which may indicate post-exploitation command execution (T1059, T1133). No public IOCs or exploitation signatures have been confirmed as of disclosure.
3. Step 3: Eradication, Apply available PAN-OS patches per the Palo Alto Networks PSIRT advisory for affected branches where fixes are published. For branches without patches yet available, maintain DNS Proxy disabled on externally facing interfaces and monitor the PSIRT advisory page for patch availability updates. Upgrade path should target the patched maintenance release within each active branch (10.2.x, 11.1.x, 11.2.x, 12.1.x) as published by Palo Alto Networks PSIRT.
4. Step 4: Recovery, After patching, re-enable DNS Proxy only on interfaces where it is operationally required. Verify firewall process integrity via system health checks and review management logs for any anomalies during the exposure window. Confirm no unauthorized administrative accounts, certificates, or configuration changes were introduced. Re-run your firewall configuration baseline comparison against your last known-good backup.
5. Step 5: Post-Incident, Review whether DNS Proxy was enabled on externally facing interfaces as a deliberate configuration or by default drift. Assess whether firewall management interfaces are adequately segmented from untrusted networks. Consider adding DNS Proxy exposure to your next firewall hardening review cycle, referencing CIS Benchmarks for Palo Alto Networks PAN-OS and NIST SP 800-41 (Guidelines on Firewalls and Firewall Policy) for control improvement baseline.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and initiate formal incident declaration if: (1) dnsproxyd core dumps are found predating your containment action, indicating active or attempted exploitation; (2) unauthorized administrative accounts, certificates, or configuration changes are discovered during recovery validation; or (3) anomalous outbound connections from firewall management IPs are identified in NetFlow or perimeter logs, indicating successful RCE and potential C2 establishment — any of these conditions elevate this from vulnerability response to confirmed security incident requiring breach notification assessment.

Recovery Notes	After applying PAN-OS patches from the Palo Alto Networks PSIRT advisory for CVE-2026-0264, re-enable DNS Proxy only on interfaces with a documented operational requirement, and verify dnsproxyd process stability via 'show system resources' over a 24-hour monitoring window to confirm no residual instability. Monitor management logs and traffic logs for 30 days post-patch for any late-stage indicators of compromise from the exposure window, specifically anomalous outbound connections from firewall process IPs or unexpected admin account activity. If core dumps or unauthorized configuration changes were found during recovery validation, treat the affected firewall as potentially compromised and consider a full factory reset and configuration rebuild from a known-good pre-exposure backup rather than patching in place.
Forensic Artifacts	dnsproxyd core dump files in /var/cores/ on PAN-OS filesystem — a heap-based buffer overflow in the DNS Proxy component may cause dnsproxyd to crash and generate a core file; presence of core dumps dated before your containment action is a primary indicator of exploitation attempts against CVE-2026-0264 | PAN-OS system log entries (Monitor > System) filtered for 'dnsproxyd', 'crash', 'restart', or 'segfault' — abnormal dnsproxyd restarts on PA-Series or VM-Series firewalls running affected PAN-OS versions (10.2, 11.1, 11.2, 12.1) during the exposure window indicate the buffer overflow trigger was reached | Traffic logs (Monitor > Traffic) showing high-volume or anomalously large DNS queries (port 53 UDP/TCP) destined for data-plane interfaces with DNS Proxy enabled — malformed oversized DNS payloads consistent with a heap overflow trigger attempt will appear as large-byte DNS sessions from external source IPs | PAN-OS running configuration XML diff against last known-good backup, specifically examining /config/mgt-config/users (admin accounts), /config/shared/certificate (certificates), and /config/devices/entry/vsys/entry/rulebase (security policy) for unauthorized additions or modifications introduced post-exploitation via RCE | 'show session all' and NetFlow/traffic log records of outbound connections initiated FROM the PA-Series firewall management or data-plane IP addresses to external destinations following DNS Proxy activity — successful RCE exploitation would manifest as the firewall itself initiating outbound sessions (MITRE ATT&CK T1059, T1133), which is anomalous for a perimeter device and constitutes a high-confidence post-exploitation indicator

Per-Action IR Details

Step 1: Containment — Identify all PA-Series hardware and VM-Series firewalls running PAN-OS 10.2, 11.1, 11.2, or 12.1. Immediately disable DNS Proxy on any interface directly reachable from the internet if DNS Proxy is not operationally required. Restrict DNS Proxy access to trusted internal segments via security policy until patches are applied. Reference: Palo Alto Networks advisory at security.paloaltonetworks.com/CVE-2026-0264 for interface-specific mitigation guidance.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 12.2 — Establish and Maintain a Secure Network Architecture (restrict DNS Proxy exposure to trusted zones)

Compensating: Run 'show system info' and 'show interface all' via SSH on each PA-Series device to enumerate PAN-OS version and interface state. Use 'show dns-proxy all' to confirm DNS Proxy status per interface. For VM-Series, query Panorama or local management console if Panorama is unavailable. A 2-person team can script this across devices using paramiko (Python SSH library) with a host list file to collect output centrally before making config changes.

Evidence: Before disabling DNS Proxy, capture: (1) 'show dns-proxy statistics' output to establish baseline request counts and any anomalous error counters; (2) current running configuration export via 'scp export configuration from

running-config.xml' to preserve the pre-change state; (3) 'show system resources' and 'show system disk-space' to detect any unusual memory or disk utilization consistent with heap exploitation. These snapshots document the firewall state at the moment of containment action and may reveal pre-exploitation artifacts.

Step 2: Detection — Query firewall management logs and system logs for unexpected process crashes or restarts in the DNS Proxy service (dnsproxyd). Review traffic logs for high-volume or malformed DNS request patterns directed at PA-Series management or data-plane interfaces with DNS Proxy enabled. Check for anomalous outbound connections from firewall processes post-DNS activity, which may indicate post-exploitation command execution (T1059, T1133). No public IOCs or exploitation signatures have been confirmed as of disclosure.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), MITRE ATT&CK T1059 (Command and Scripting Interpreter) — post-exploitation code execution via compromised firewall process, MITRE ATT&CK T1133 (External Remote Services) — adversary maintaining access through compromised perimeter device

Compensating: Without a SIEM, extract PAN-OS system logs directly: navigate to Monitor > System in the PAN-OS web UI and filter for 'dnsproxyd' process events, or use CLI: 'show log system direction equal backward' and grep for 'crash', 'restart', or 'core'. For traffic log analysis of malformed DNS, use 'show log traffic' filtered on destination port 53 with unusually large payload sizes or high request rates from a single source. Capture raw packet data on the management interface using 'debug dataplane packet-diag' if exploitation is suspected. Use Wireshark to inspect any pcap exports for DNS query anomalies such as oversized QNAME fields or unexpected opcode values that would trigger the heap overflow in dnsproxyd.

Evidence: Before analysis, preserve: (1) PAN-OS system log export filtered for dnsproxyd process events from the 30 days prior to disclosure (May 13, 2026) to identify any pre-patch exploitation — accessible via Monitor > System > Export to CSV; (2) traffic logs showing DNS traffic (port 53 UDP/TCP) to data-plane interfaces with DNS Proxy enabled, specifically large-payload DNS queries that may represent overflow trigger attempts; (3) any core dump files generated by dnsproxyd crashes, located in /var/cores/ on the PAN-OS filesystem, accessible via 'show system files' and SCP export; (4) 'show session all' output captured at time of suspected exploitation to identify anomalous sessions established from the firewall itself post-DNS activity, which would indicate successful RCE and outbound C2.

Step 3: Eradication — Apply available PAN-OS patches per the Palo Alto Networks advisory for affected branches where fixes are published. For branches without patches yet available, maintain DNS Proxy disabled on externally facing interfaces and monitor the PSIRT advisory page for patch availability updates. Upgrade path should target the patched maintenance release within each active branch (10.2.x, 11.1.x, 11.2.x, 12.1.x) as published by Palo Alto Networks PSIRT.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Monitor https://security.paloaltonetworks.com/CVE-2026-0264 directly (bookmark and check daily) for patch availability per branch. Before applying any PAN-OS maintenance release, verify the software image hash against Palo Alto Networks published checksums using 'verify software version' in the PAN-OS CLI after download — do not skip this step, as a compromised firewall could serve a tampered image. For VM-Series firewalls, take a hypervisor-level snapshot before upgrading to preserve a forensically clean pre-patch state. Stage upgrades on non-production devices first within each branch (10.2.x, 11.1.x, 11.2.x, 12.1.x) to verify no regression before pushing to perimeter devices.

Evidence: Before patching, export: (1) full running configuration ('scp export configuration') as a forensic baseline showing any unauthorized changes introduced during the exposure window since initial deployment on the affected

PAN-OS version; (2) 'show system info' output documenting exact current PAN-OS version, serial number, and uptime — unexpectedly short uptime may indicate a prior crash or forced restart consistent with exploitation attempts; (3) administrator account list via 'show admins' and 'show config running | match admin' to identify any accounts not present in your change management records, which would indicate post-exploitation persistence (MITRE ATT&CK T1136 — Create Account).

Step 4: Recovery — After patching, re-enable DNS Proxy only on interfaces where it is operationally required. Verify firewall process integrity via system health checks and review management logs for any anomalies during the exposure window. Confirm no unauthorized administrative accounts, certificates, or configuration changes were introduced. Re-run your firewall configuration baseline comparison against your last known-good backup.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST CM-3 (Configuration Change Control), NIST IA-5 (Authenticator Management), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Use the PAN-OS CLI command 'show config running | match admin' and compare output against your change-controlled account inventory to detect any unauthorized admin accounts created during the exposure window. Verify certificates via 'show certificate-info' and cross-reference against your PKI records for any certificates enrolled without authorization. Use 'show system resources' and 'show system health' post-patch to confirm dnsproxyd is running normally without elevated memory consumption. If you maintain configuration backups in a version-controlled repository (even a simple Git repo with exported XML configs), run a diff against the pre-incident baseline to surface any unauthorized policy or object changes.

Evidence: Before re-enabling DNS Proxy, collect: (1) post-patch 'show system info' confirming the patched PAN-OS version is active; (2) full configuration export post-patch for diff comparison against the pre-exposure-window baseline — pay specific attention to admin accounts (xpath: /config/mgt-config/users), certificates (xpath: /config/shared/certificate), and security policy rules that may have been altered; (3) 'show log system' entries covering the full exposure window between the earliest affected PAN-OS deployment and patch application, archived to an external log repository per NIST AU-11 (Audit Record Retention) requirements; (4) 'show session info' to confirm no persistent sessions remain from IP addresses identified as anomalous during detection phase.

Step 5: Post-Incident — Review whether DNS Proxy was enabled on externally facing interfaces as a deliberate configuration or by default drift. Assess whether firewall management interfaces are adequately segmented from untrusted networks. Consider adding DNS Proxy exposure to your next firewall hardening review cycle, referencing CIS Benchmarks for Palo Alto Networks PAN-OS and NIST SP 800-41 (Guidelines on Firewalls and Firewall Policy) for control improvement baseline.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST CM-6 (Configuration Settings), NIST CM-8 (System Component Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Conduct a post-incident lessons-learned meeting within 5 business days of patch completion. Document: (1) how many PA-Series and VM-Series firewalls had DNS Proxy enabled on external interfaces at time of disclosure, and whether this was intentional or configuration drift; (2) mean time from disclosure (May 13, 2026) to containment action (DNS Proxy disabled) per device, to establish a remediation SLA benchmark for future perimeter device vulnerabilities; (3) whether your asset inventory (CIS 1.1) accurately reflected all PAN-OS versions in production, since the discovery step in this incident should have been automated. Add a DNS Proxy enabled/disabled check to your quarterly PAN-OS hardening review using 'show dns-proxy all' output, and document the expected state per interface in your configuration baseline.

Evidence: Retain for post-incident review: (1) the full timeline of detection-to-containment events reconstructed from system logs and change management records, to measure response SLA against NIST IR-8 (Incident Response Plan) benchmarks; (2) a complete inventory of all PA-Series and VM-Series devices showing PAN-OS version, DNS Proxy state, and interface exposure at time of disclosure — this inventory gap analysis feeds directly into CIS 1.1 and CIS 2.2 remediation; (3) archived configuration diffs from the exposure window showing any unauthorized changes, retained per NIST AU-11 (Audit Record Retention) and your records retention policy, in the event regulatory notification or forensic review is required later.

Detection Guidance

No confirmed public exploitation signatures or IOCs exist as of the May 13, 2026 disclosure date. Establish baseline DNS traffic and dnsproxyd process behavior on your PA-Series devices immediately to enable faster detection of any exploitation attempts during the exposure window. Detection should focus on behavioral indicators. On affected PA-Series devices: monitor system logs for unexpected termination or restart of the dnsproxyd process; this is the most direct indicator of exploitation attempts triggering the overflow. Review PAN-OS traffic logs for high-rate or structurally anomalous DNS queries targeting interfaces where DNS Proxy is enabled, particularly from external or untrusted source IPs. Post-exploitation indicators aligned to mapped MITRE techniques include: unexpected outbound connections from the firewall to external IPs (T1133), unusual command execution artifacts in process logs (T1059), and degraded forwarding performance consistent with T1499 (denial of service as a side effect of failed exploitation). If your SIEM ingests PAN-OS syslog, create alerts on dnsproxyd crash events and correlated spikes in DNS traffic volume from single external sources. Threat hunting hypothesis: PA-Series firewall with DNS Proxy enabled receives sustained DNS request volume from a single external IP, followed within minutes by a process restart event or an outbound connection to a non-DNS external host.

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1499** — Endpoint Denial of Service
- **T1203** — Exploitation for Client Execution
- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter

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
- **SC-5** — Denial-of-Service Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection

- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-7** — Least Functionality
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1133	External Remote Services	Persistence
T1499	Endpoint Denial of Service	Impact
T1203	Exploitation for Client Execution	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
Palo Alto Networks Security Advisories	https://security.paloaltonetworks.com/CVE-2026-0264	T3
CVE-2026-26264 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-26264	T1

Source	URL	Tier
TencentOS Server 2: python3 (TSSA-2026:0264) | Tenable®	https://www.tenable.com/plugins/nessus/310952	T3
ZDI-26-264 - Zero Day Initiative	https://www.zerodayinitiative.com/advisories/ZDI-26-264/	T3
CVE-2026-2664: Docker Desktop Privilege Escalation Flaw	https://www.sentinelone.com/vulnerability-database/cve-2026-2664/	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-0264	T1

Generated 2026-05-13 14:28 UTC by TJS Security Command Center