INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-15 19:02 UTC

PAN-OS DoS Vulnerabilities Allow Unauthenticated Dataplane Crash Across Four Version Branches (CVE-2026-0262)

CVE VULNERABILITY | MEDIUM | CVSS 5.0

SCC Item ID	SCC-CVE-2026-0186
Type	CVE Vulnerability
CVE ID	CVE-2026-0262
Severity	MEDIUM
CVSS Base Score	5.0
EPSS Score	0.0005 (16th percentile)
Affected Products	Palo Alto Networks PAN-OS 10.2, 11.1, 11.2, 12.1; Prisma Access (patched as of 2026-05-15); Cloud NGFW unaffected; Panorama unaffected
Published	2026-05-15T19:15:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

Palo Alto Networks disclosed CVE-2026-0262, a denial-of-service vulnerability affecting PAN-OS versions 10.2, 11.1, 11.2, and 12.1. An unauthenticated attacker on the same network can crash the firewall dataplane by sending crafted packets, with no special configuration required. No active exploitation has been reported; however, the broad version coverage and zero-authentication requirement make patching a priority for any organization running affected PAN-OS branches.

Technical Analysis

CVE-2026-0262 is a set of denial-of-service vulnerabilities in PAN-OS network traffic parsing logic (CWE-754: Improper Check for Unusual or Exceptional Conditions). An unauthenticated, network-adjacent attacker can send specially crafted packets to crash the dataplane, the forwarding and security inspection plane, rendering the device unable to process traffic. Affected branches: PAN-OS 10.2, 11.1, 11.2, and 12.1. No special configuration is required for exposure. CVSS base score: 5.0 (Medium). EPSS: 0.051% probability (16th percentile). Prisma Access was proactively patched as of 2026-05-15. Cloud NGFW and Panorama are not affected. Some fixes for on-premises PAN-OS branches remain pending release per the advisory. No active exploitation has been reported. MITRE techniques: T1499 (Endpoint Denial of Service), T1498 (Network Denial of Service), T1499.004 (Application or System Exploitation). Source: Palo Alto Networks PSIRT advisory.

Action Checklist

1. Containment: Inventory all PAN-OS devices running versions 10.2, 11.1, 11.2, or 12.1 and identify which are network-adjacent to untrusted segments or internet-facing. Restrict management and dataplane access to trusted source IPs via security policy where operationally feasible while patches are prepared.
2. Detection: Query your asset management and Panorama (if in use) for PAN-OS version strings matching affected branches. Review firewall syslog and PAN-OS system logs for unexpected dataplane process restarts (event type: 'dataplane restart' or 'dp-monitor' events). Elevated restart counts without known cause warrant investigation.
3. Eradication: Apply Palo Alto Networks-issued fixes for CVE-2026-0262 per the vendor advisory at https://security.paloaltonetworks.com/CVE-2026-0262 as patches become available for each branch. Prisma Access customers require no action; remediation was applied 2026-05-15. Confirm target fix versions per branch in the PSIRT advisory before upgrading.
4. Recovery: After patching, validate dataplane stability by confirming normal traffic forwarding resumes and no unexpected process restarts occur. Monitor PAN-OS system logs for 24-48 hours post-patch. Verify security policy enforcement is intact and threat prevention profiles remain active.
5. Post-Incident: Document which PAN-OS branches in your environment had delayed patch coverage and why. Review patch cadence SLAs for perimeter firewall infrastructure. Evaluate whether network segmentation adequately limits unauthenticated adjacency to firewall dataplanes from untrusted hosts.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to Palo Alto Networks TAC and initiate formal incident handling if any affected PAN-OS device (running 10.2, 11.1, 11.2, or 12.1) records more than one unexpected 'dp-monitor' or 'dataplane restart' event within a short window while network-adjacent to untrusted hosts — this pattern is a high-confidence indicator of active CVE-2026-0262 exploitation and may trigger breach notification obligations if the firewall protects environments subject to HIPAA, PCI-DSS, or similar regulatory frameworks.
Recovery Notes	After applying the Palo Alto Networks-issued fix for CVE-2026-0262, validate dataplane stability by polling 'show dp-monitor statistics' at regular intervals for a minimum of 48 hours and confirming the restart counter does not increment. Re-verify that threat prevention profiles and security policies are fully intact and enforcing as expected on all previously affected devices, since a destabilized dataplane may have disrupted policy enforcement during any exploitation window. If your environment spans multiple PAN-OS branches (e.g., both 10.2 and 11.2), sequence patch deployment and recovery validation per branch and do not close the incident until all affected branches are confirmed patched and stable.

Forensic Artifacts	PAN-OS System Logs (Monitor > Logs > System, or /var/log/pan/system on device filesystem): Filter for event keywords 'dp-monitor', 'dataplane restart', and severity 'critical' — these are the primary indicators of CVE-2026-0262 being triggered, as the vulnerability mechanism crashes the dataplane process and PAN-OS logs the restart event with a timestamp. | PAN-OS Traffic Logs (Monitor > Logs > Traffic) for interfaces adjacent to untrusted zones: Capture all sessions in the 5-minute window preceding any dataplane restart event — the crafted packets used to trigger the CVE-2026-0262 DoS will appear as anomalous inbound sessions, potentially with malformed or truncated packet indicators, from source IPs on the same network segment as the affected dataplane interface. | 'show dp-monitor statistics' CLI output (timestamped captures): This command reveals dataplane process restart counts and timing with precision; sequential captures showing an incrementing restart counter on an unpatched device adjacent to untrusted hosts is direct forensic evidence of active exploitation of CVE-2026-0262. | 'show system info' CLI output: Documents the exact PAN-OS software version string running at the time of any suspected exploitation event — critical for confirming the device was running a vulnerable branch (10.2, 11.1, 11.2, or 12.1) and for the post-incident record establishing patch status at time of incident. | Network packet capture (PCAP) on the ingress interface adjacent to untrusted segments (captured via 'debug dataplane packet-diag' or a tap/span port with Wireshark): Preserving the raw packet stream in the window surrounding a dataplane restart event may capture the crafted packets used to trigger CVE-2026-0262, providing the highest-fidelity forensic evidence of exploitation and supporting threat intelligence sharing with Palo Alto Networks PSIRT.

Per-Action IR Details

Containment — Inventory all PAN-OS devices running versions 10.2, 11.1, 11.2, or 12.1 and identify which are network-adjacent to untrusted segments or internet-facing. Restrict management and dataplane access to trusted source IPs via security policy where operationally feasible while patches are staged.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run 'show system info | match sw-version' via SSH on each PAN-OS device to enumerate version strings without Panorama. For access restriction without a SIEM, create a PAN-OS security policy zone-based rule permitting only your management jump host CIDR to the dataplane interfaces; use 'show security policy-statistics' to confirm enforcement. Document all device IPs and versions in a flat spreadsheet as your interim asset inventory.

Evidence: Before restricting access, capture 'show system resources' and 'show interface all' outputs to establish a pre-containment baseline of dataplane CPU/memory utilization and interface states. Export the current running security policy via 'show running security-policy' so any attacker-modified policies can be identified after containment. Record interface adjacency (which untrusted VLANs or zones are directly routed to each affected PAN-OS dataplane) — this defines the blast radius for CVE-2026-0262 exploitation, which requires only same-network adjacency with crafted packets and no authentication.

Detection — Query your asset management and Panorama (if in use) for PAN-OS version strings matching affected branches. Review firewall syslog and PAN-OS system logs for unexpected dataplane process restart events (event type: 'dataplane restart' or 'dp-monitor' events). Elevated restart counts without known cause warrant investigation.

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 IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without Panorama, SSH to each affected device and run 'show log system direction equal backward | match dp-monitor' and 'show log system direction equal backward | match dataplane' to retrieve recent dataplane restart events from the local system log. For version enumeration across many devices, write a bash loop using sshpass or Ansible ad-hoc to collect 'show system info' output from each firewall IP in a target list. Forward PAN-OS syslog (facility local0, severity critical/error) to a free syslog aggregator such as rsyslog or Graylog CE and grep for the string 'dp-monitor' or 'dataplane restart' to identify anomalous restart counts. A single unexpected dataplane restart on an unpatched device adjacent to an untrusted segment is a high-confidence indicator of CVE-2026-0262 exploitation.

Evidence: Collect PAN-OS system logs (Monitor > Logs > System in the GUI, or /var/log/pan/system on the device filesystem) filtered for event types 'dp-monitor', 'dataplane', and 'critical' within the 72-hour window preceding detection. Export traffic logs (Monitor > Logs > Traffic) for inbound sessions on interfaces adjacent to untrusted zones immediately preceding any restart event — the crafted packets triggering CVE-2026-0262 may appear as anomalous or malformed sessions. Capture 'show system statistics' and 'show dp-monitor statistics' CLI output to document restart counts and timestamps as forensic evidence of exploitation attempts.

Eradication — Apply Palo Alto Networks-issued fixes for CVE-2026-0262 per the vendor advisory at https://security.paloaltonetworks.com/CVE-2026-0262 as patches become available for each branch. Prisma Access customers require no action — remediation was applied 2026-05-15. Confirm target fix versions per branch in the PSIRT advisory before upgrading.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), 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: Without an enterprise patch management platform, stage PAN-OS software images manually via the device web UI (Device > Software) or CLI ('request system software download version ') using the exact fixed version strings published in the Palo Alto PSIRT advisory for each affected branch (10.2.x, 11.1.x, 11.2.x, 12.1.x). Verify image integrity using the SHA-256 hash published in the advisory before installation. Maintain a patch tracking spreadsheet recording device hostname, current version, target version, patch date, and the technician who applied it — this is your audit trail for NIST SI-2 compliance. For Prisma Access, validate remediation by checking the Prisma Access Cloud Management console for the applied software version dated 2026-05-15 or later.

Evidence: Before upgrading, export a full device configuration backup ('save config to .xml') and capture 'show system info' output to document the pre-patch version string as a forensic baseline. After upgrade, capture 'show system info' again to confirm the fixed version is running and retain both outputs. If any dataplane restarts occurred prior to patching, preserve the full PAN-OS system log export from that window — this log is the primary forensic record of whether CVE-2026-0262 was actively triggered in your environment and may be required for incident documentation under NIST IR-6 (Incident Reporting).

Recovery — After patching, validate dataplane stability by confirming normal traffic forwarding resumes and no unexpected process restarts occur. Monitor PAN-OS system logs for 24-48 hours post-patch. Verify security policy enforcement is intact and threat prevention profiles remain active.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Run 'show system resources' and 'show dp-monitor statistics' every 15 minutes for the first 2 hours post-patch to confirm dataplane process stability and zero restart events. Use 'show running security-policy' and compare output against your pre-patch baseline capture to detect any policy drift. Verify threat prevention profiles are

active with 'show profiles threat' and confirm Security Profiles are attached to all internet-facing and untrusted-zone policies. Without a dedicated monitoring platform, set a cron job or scheduled task to SSH-poll 'show dp-monitor statistics' every 5 minutes for the first 24 hours and alert on any non-zero restart delta.

Evidence: Capture 'show system info', 'show dp-monitor statistics', 'show system resources', and 'show security policy-statistics' immediately after patch completion and at 1-hour, 4-hour, 12-hour, and 24-hour intervals — these time-stamped outputs are your recovery verification record demonstrating the dataplane stabilized post-fix and no exploitation of CVE-2026-0262 recurred. Retain all system log exports from the 24-48 hour monitoring window as evidence that no further 'dp-monitor' or 'dataplane restart' events occurred after the patched version was confirmed running.

Post-Incident — Document which PAN-OS branches in your environment had delayed patch coverage and why. Review patch cadence SLAs for perimeter firewall infrastructure. Evaluate whether network segmentation adequately limits unauthenticated adjacency to firewall dataplanes from untrusted hosts.

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 RA-3 (Risk Assessment), 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: Produce a one-page lessons-learned document covering: (1) how many PAN-OS devices per branch were unpatched at disclosure, (2) time-to-patch per branch, (3) whether any dp-monitor restart events were observed that could indicate exploitation, and (4) which untrusted network segments were adjacent to unpatched dataplane interfaces. Use this document to drive a 30-day review of your firewall patch SLA — for perimeter devices running PAN-OS, a CVSS 5.0 unauthenticated DoS with broad version coverage warrants a patch window of no more than 14 days from vendor advisory. Evaluate network topology diagrams to identify any hosts in untrusted zones with layer-2 or layer-3 adjacency to PAN-OS dataplane interfaces and add VLAN isolation or ACLs as compensating controls for future exposure.

Evidence: Preserve the full incident timeline: Palo Alto PSIRT advisory publication date, internal detection date, containment date per device, patch date per device, and recovery validation date. Retain all system log exports, configuration backups, and CLI output captures collected during the incident as your post-incident evidence package. If any unexplained dataplane restarts were observed on affected devices adjacent to untrusted segments during the exposure window, escalate to Palo Alto Networks TAC with log exports and treat as a potential exploitation event requiring formal incident review under NIST IR-6 (Incident Reporting).

Detection Guidance

Query Panorama or individual device logs for dataplane restart events ('dp-monitor' or 'dataplane' process exit/restart entries in the system log). In PAN-OS, navigate to Monitor > Logs > System and filter for severity 'critical' or event descriptions referencing dataplane or dp-monitor. Baseline normal restart frequency first; a sudden increase, especially correlated with traffic anomalies, warrants review. No public IOC patterns (IP, hash, domain) have been reported for this vulnerability. Network-level detection: IDS/IPS rules targeting malformed or anomalous packet patterns in protocols handled by PAN-OS parsing logic may provide early warning, but no specific signatures have been published as of the Palo Alto Networks advisory date.

Framework Mappings

MITRE-ATTACK

- **T1499** — Endpoint Denial of Service
- **T1498** — Network Denial of Service

- **T1499.004** — Application or System Exploitation

NIST-800-53R5

- **SC-5** — Denial-of-Service Protection
- **IR-5** — Incident Monitoring

CIS-V8

- **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.5.23** — 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
T1499	Endpoint Denial of Service	Impact
T1498	Network Denial of Service	Impact
T1499.004	Application or System Exploitation	Impact

Sources

Source	URL	Tier
Palo Alto Networks Security Advisories	https://security.paloaltonetworks.com/CVE-2026-0262	T3
CVE-2026-0262 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-0262	T1
CVE-2026-0262 | Tenable®	https://www.tenable.com/cve/CVE-2026-0262	T3
CVE Record: CVE-2026-0262 - Palo Alto Networks, Inc.	https://www.cve.org/CVERecord?id=CVE-2026-0262	T3
CVE-2026-0262 Security Vulnerability Analysis & Exploit Details	https://cve.akaoma.com/cve-2026-0262	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-15 19:02 UTC by TJS Security Command Center