INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-09 06:35 UTC

CVE-2026-0288: Unauthenticated Buffer Overflow in PAN-OS TSA Threatens Enterprise Firewall Integrity

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0399
Type	CVE Vulnerability
CVE ID	CVE-2026-0288
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Palo Alto Networks PAN-OS 10.2, 11.1, 11.2, 12.1; Prisma Access 10.2, 11.2; Cloud NGFW (unaffected)
Published	2026-07-08T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

Palo Alto Networks disclosed CVE-2026-0288 on July 8, 2026, a set of buffer overflow vulnerabilities in the User-ID Terminal Server Agent (TSA) component affecting PAN-OS versions 10.2 through 12.1 and Prisma Access. An unauthenticated attacker with network access to the TSA service can trigger denial of service or, according to the advisory, potentially achieve arbitrary code execution. Organizations running affected PAN-OS versions should treat this as a priority patching event given the broad version coverage and the unauthenticated attack surface.

Technical Analysis

CVE-2026-0288 covers multiple memory corruption weaknesses in the PAN-OS User-ID Terminal Server Agent (TSA): CWE-787 (out-of-bounds write), CWE-120 (classic buffer overflow), and CWE-119 (improper restriction of operations within a memory buffer). An unauthenticated attacker with network-layer access to the TSA service can send crafted traffic to trigger these conditions, resulting in denial of service or potentially arbitrary code execution. Affected platforms: PAN-OS 10.2, 11.1, 11.2, 12.1; Prisma Access 10.2 and 11.2. Cloud NGFW is confirmed unaffected per the Palo Alto Networks advisory. CVSS base score: 7.5 (High). MITRE technique mapping includes T1190 (Exploit Public-Facing Application), T1499 (Endpoint Denial of Service), T1059 (Command and Scripting Interpreter), and T1203 (Exploitation for Client Execution). No exploitation in the wild was confirmed in the source material at time of writing; current KEV status should be verified directly against the

CISA KEV catalog and Palo Alto Networks PSIRT advisory.

Action Checklist

1. Step 1: Containment. Identify all systems running PAN-OS 10.2, 11.1, 11.2, or 12.1, and Prisma Access 10.2 or 11.2. Immediately restrict network access to the TSA service port (default: 5007; verify in your environment) from untrusted or internet-facing segments. Confirm Cloud NGFW deployments are unaffected and deprioritize those from the queue. Reference the Palo Alto Networks PSIRT advisory at https://security.paloaltonetworks.com/CVE-2026-0288 for TSA port specifics and interim mitigations.
2. Step 2: Detection. Query firewall and TSA service logs for anomalous or malformed traffic targeting the TSA listener. Look for unexpected process crashes, restarts, or memory fault events in PAN-OS system logs (event categories: system, threat). Review SIEM for high-volume or structurally malformed connections to the TSA port from untrusted sources. Align log collection with NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). No confirmed IOCs were present in the source material at time of writing.
3. Step 3: Eradication. Apply vendor-issued patches for affected PAN-OS branches (10.2, 11.1, 11.2, 12.1) and Prisma Access (10.2, 11.2) per the Palo Alto Networks PSIRT advisory. Patch version specifics should be sourced directly from https://security.paloaltonetworks.com/CVE-2026-0288. If patching cannot be completed immediately, disable or restrict TSA service access as an interim measure per vendor guidance.
4. Step 4: Recovery. After patching, validate TSA service stability and confirm no residual crash or restart events in system logs. Re-enable any restricted network segments in a staged manner. Monitor TSA and PAN-OS logs for 72 hours post-remediation for anomalous behavior. Verify EPSS and CISA KEV status at https://www.cisa.gov/known-exploited-vulnerabilities-catalog to confirm no exploitation activity emerged during the remediation window. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) for post-patch log review.
5. Step 5: Post-Incident. Review network segmentation controls to assess whether TSA service exposure was broader than operationally required (NIST AC-4, Information Flow Enforcement; CIS 4.4, Implement and Manage a Firewall on Servers). Evaluate whether TSA is required across all affected branches or whether scope can be reduced. Document patch timelines and gaps for future audit preparation. Confirm audit logging coverage of TSA events meets NIST AU-2 and AU-12 requirements.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to senior IR leadership and legal/compliance if PAN-OS system logs or TSA agent crash dumps show evidence of successful arbitrary code execution (not merely DoS) on a firewall enforcing PII, PHI, PCI, or critical infrastructure traffic segments, as exploitation of the management plane may constitute a reportable breach under HIPAA, PCI DSS, or sector-specific regulations.

Recovery Notes	After applying Palo Alto Networks PSIRT-specified patches for each affected PAN-OS branch (10.2, 11.1, 11.2, 12.1) and Prisma Access (10.2, 11.2), validate TSA service stability by confirming absence of useridd crash events in PAN-OS system logs and Event ID 1000/1001 absence on Windows TSA agent hosts for a minimum 72-hour post-patch observation window. Re-enable previously restricted network segments to the TSA listener in staged increments — one zone at a time — verifying User-ID IP mapping function is operating correctly before proceeding. Monitor CISA KEV and Palo Alto Networks PSIRT for any update to CVE-2026-0288 exploitation status that would require re-escalation of the incident severity.
Forensic Artifacts	PAN-OS system log entries for the 'useridd' (User-ID daemon) process — specifically crash, restart, and fault events — exported via 'scp export log system' from the PAN-OS CLI, covering the 72-hour window preceding detection of anomalous TSA behavior. | Windows Application Event Log (Application.evtx) from TSA agent hosts, filtered for Event ID 1000 (Application Error) and Event ID 1001 (Windows Error Reporting) with FaultingApplicationName matching the Palo Alto Networks TSA executable, indicating buffer overflow-triggered process crashes. | Full packet capture (PCAP) of traffic to TCP 5009 (TSA listener port) captured via tcpdump or Wireshark prior to containment actions — to be analyzed for malformed or oversized User-ID protocol frames consistent with buffer overflow exploitation attempts against CVE-2026-0288. | Memory dump of the TSA agent process captured via ProcDump before any patch or service termination, preserving heap and stack state that may contain exploit shellcode, return-oriented programming chains, or attacker-controlled data introduced through the buffer overflow. | TSA agent configuration files and agent-side logs from C:\Program Files\Palo Alto Networks\Terminal Server Agent\ on Windows agent hosts, which may record connection attempts, authentication failures, or protocol errors generated during exploitation reconnaissance or active attack.

Per-Action IR Details

Step 1: Containment — Identify all systems running PAN-OS 10.2, 11.1, 11.2, or 12.1, and Prisma Access 10.2 or 11.2. Immediately restrict network access to the TSA service port from untrusted or internet-facing segments. Confirm Cloud NGFW deployments are unaffected and deprioritize those from the queue. Reference the Palo Alto Networks PSIRT advisory at https://security.paloaltonetworks.com/CVE-2026-0288 for TSA port specifics and interim mitigations.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'show system info | match sw-version' via PAN-OS CLI across all managed firewalls to enumerate affected version branches (10.2, 11.1, 11.2, 12.1); for Prisma Access, check the Cloud Management portal tenant version. Block inbound connections to the TSA listener port (default TCP 5009) from untrusted segments using a host-based ACL or upstream perimeter rule — use 'iptables -I INPUT -p tcp --dport 5009 -s -j DROP' on any Linux-based management host proxying TSA traffic, or apply a PAN-OS Security Policy rule denying untrusted source zones to the TSA service object.

Evidence: Before restricting TSA port access, capture active TCP connection state to the TSA listener: run 'netstat -ano | findstr :5009' (Windows TSA agent host) or 'ss -tnp sport = :5009' (Linux) to enumerate current sessions and associated PIDs. Capture the TSA process memory dump using ProcDump ('procdump -ma tsa_pre_containment.dmp') if the agent is running on a Windows host, preserving any in-memory exploit artifacts before ACL changes terminate live connections. Document all external source IPs connected to TSA at time of containment.

Step 2: Detection — Query firewall and TSA service logs for anomalous or malformed traffic targeting the TSA listener. Look for unexpected process crashes, restarts, or memory fault events in PAN-OS system logs

(event categories: system, threat). Review SIEM for high-volume or structurally malformed connections to the TSA port from untrusted sources. Align log collection with NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). No confirmed IOCs were present in the source material at time of writing.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: On the PAN-OS management plane, run 'show log system direction equal forward category equal system' filtered for 'useridd' (User-ID daemon) crash or restart events — TSA crashes triggered by CVE-2026-0288 exploitation will appear as useridd process faults. On the Windows TSA agent host, query the Windows Event Log for Event ID 1000 (Application Error) and Event ID 1001 (Windows Error Reporting) with FaultingApplicationName matching the PAN TSA executable. Use Wireshark or tcpdump ('tcpdump -i tcp port 5009 -w tsa_capture.pcap') to capture raw traffic to the TSA listener and inspect for oversized or malformed User-ID protocol frames indicative of buffer overflow attempts.

Evidence: Before any containment action that terminates connections, preserve: (1) PAN-OS system log entries for the 'useridd' process covering the 72-hour window preceding detection — export via 'scp export log system' from the PAN-OS CLI; (2) TSA agent application event logs from the Windows host (%SystemRoot%\System32\winevt\Logs\Application.evtx); (3) a full packet capture of traffic to TCP 5009 showing connection volume, source distribution, and frame structure to identify malformed User-ID protocol messages consistent with buffer overflow payloads.

Step 3: Eradication — Apply vendor-issued patches for affected PAN-OS branches (10.2, 11.1, 11.2, 12.1) and Prisma Access (10.2, 11.2) per the Palo Alto Networks PSIRT advisory. Patch version specifics should be sourced directly from https://security.paloaltonetworks.com/CVE-2026-0288. If patching cannot be completed immediately, disable or restrict TSA service access as an interim measure per vendor guidance.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For teams unable to patch immediately, disable the TSA service on the Windows agent host via 'sc stop "Palo Alto Networks Terminal Server Agent" && sc config "Palo Alto Networks Terminal Server Agent" start= disabled' and validate cessation with 'sc query'. On the PAN-OS side, navigate to Device > User Identification > Terminal Server Agents and remove or disable all TSA agent entries to sever the management plane's acceptance of TSA connections. Document the interim disable action with timestamp for audit trail.

Evidence: Before applying any patch or disabling the TSA service — both of which alter live system state — capture: (1) a full memory dump of the TSA agent process ('procdump -ma tsa_pre_patch.dmp') to preserve any evidence of prior exploitation attempts residing in heap or stack memory; (2) current TSA agent configuration files (typically under C:\Program Files\Palo Alto Networks\Terminal Server Agent\) including agent logs and configuration XML; (3) 'netstat -ano' output from the TSA host timestamped immediately before patching to record any active connections at time of eradication. These captures must occur before the patch installer terminates the service.

Step 4: Recovery — After patching, validate TSA service stability and confirm no residual crash or restart events in system logs. Re-enable any restricted network segments in a staged manner. Monitor TSA and PAN-OS logs for 72 hours post-remediation for anomalous behavior. Verify EPSS and CISA KEV status at https://www.cisa.gov/known-exploited-vulnerabilities-catalog to confirm no exploitation activity emerged during the remediation window. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) for post-patch log review.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: After patching, confirm patched version with 'show system info | match sw-version' and validate the TSA service is running cleanly via 'sc query "Palo Alto Networks Terminal Server Agent"' on the agent host. Schedule a cron job or Windows Scheduled Task to run every 15 minutes for the 72-hour watch window, writing 'netstat -ano | findstr :5009' output and Event ID 1000/1001 counts to a local log file for analyst review. Re-enable restricted segments one at a time, validating TSA connectivity and PAN-OS User-ID mapping function after each segment is restored before proceeding to the next.

Evidence: During the recovery watch window, continuously collect: (1) PAN-OS system logs filtered for 'useridd' events to confirm no post-patch process crashes; (2) TSA agent Windows Application Event Log entries for Event ID 1000/1001 to detect any instability in the newly patched binary; (3) network flow records or packet captures to TCP 5009 confirming that only authorized management-plane sources are communicating with the TSA listener post-segment re-enablement. These are monitoring artifacts, not pre-action volatile captures, but must be retained for the post-incident review.

Step 5: Post-Incident — Review network segmentation controls to assess whether TSA service exposure was broader than operationally required (NIST AC-4, Information Flow Enforcement; CIS 4.4, Implement and Manage a Firewall on Servers). Evaluate whether TSA is required across all affected branches or whether scope can be reduced. Document patch timelines and gaps for future audit preparation. Confirm audit logging coverage of TSA events meets NIST AU-2 and AU-12 requirements.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-4 (Information Flow Enforcement), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Produce a TSA exposure map by querying PAN-OS Security Policy rules ('show running security-policy') to identify any rule permitting broad or internet-sourced access to TCP 5009, and document whether the TSA deployment scope (number of agent hosts, zones served) matches current operational need. Use the PAN-OS built-in ACC (Application Command Center) or log viewer to enumerate unique source IPs that communicated with the TSA port over the past 90 days, and flag any sources outside the expected Windows domain controller or AD infrastructure range. File findings in the organization's vulnerability management tracking system with patch timeline evidence for audit use.

Evidence: Post-incident artifacts to retain for the lessons-learned record: (1) exported PAN-OS system logs covering the full incident window (useridd events); (2) TSA agent Windows Event Logs (Application.evtx) from all affected hosts; (3) the pre-patch and post-patch 'show system info' version outputs; (4) network ACL or Security Policy rule snapshots showing TSA exposure before and after containment; (5) the CISA KEV page status for CVE-2026-0288 at time of remediation completion. No volatile capture obligation applies to this phase as live state has already been stabilized.

Detection Guidance

Query PAN-OS system and threat logs for unexpected TSA process restarts, memory fault events, or crash entries following anomalous inbound connections to the TSA service port. In your SIEM, filter for high-rate or structurally irregular connections targeting the TSA listener from untrusted source IPs, particularly those originating outside expected identity infrastructure segments. Correlate with NIST AU-6 (Audit Record Review, Analysis, and Reporting) processes to flag deviations from TSA baseline traffic patterns. No confirmed IOC patterns (IPs, hashes, payloads) were present in the source material at the time of writing; consult the Palo Alto Networks PSIRT advisory directly for any updated indicators. Monitor for post-exploitation indicators including unexpected process execution, privilege escalation attempts, and lateral movement from the compromised firewall if code execution is achieved.

Framework Mappings

MITRE-ATTACK

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

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **SC-5** — Denial-of-Service Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **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.5.23** — 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
T1059	Command and Scripting Interpreter	Execution

Technique ID	Technique Name	Tactic
T1499	Endpoint Denial of Service	Impact
T1190	Exploit Public-Facing Application	Initial-Access
T1203	Exploitation for Client Execution	Execution

Sources

Source	URL	Tier
Palo Alto Networks Security Advisories	https://security.paloaltonetworks.com/CVE-2026-0288	T1
Cybersecuritynews	https://cybersecuritynews.com/palo-alto-networks-pan-os-vulnerability/	T3
CVE-2026-0288 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-0288	T1
CVE Record: CVE-2026-0288	https://www.cve.org/CVERecord?id=CVE-2026-0288	T1
Known Exploited Vulnerabilities Catalog	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1

Generated 2026-07-09 06:35 UTC by TJS Security Command Center