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

Palo Alto Trust Protection Foundation Vault Exposure Enables Full User Impersonation, Patch Now

CVE VULNERABILITY | **MEDIUM** | CVSS 5.0

SCC Item ID	SCC-CVE-2026-0171
Type	CVE Vulnerability
CVE ID	CVE-2026-0240
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Palo Alto Networks Trust Protection Foundation versions 24.1.0-24.1.12, 24.3.0-24.3.5, 25.1.0-25.1.7, 25.3.0-25.3.2
Published	2026-05-13T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

CVE-2026-0240 is an information disclosure vulnerability in Palo Alto Networks Trust Protection Foundation that allows an authenticated attacker with adjacent-network access to extract credentials from the product vault, enabling full user impersonation and unrestricted configuration modification. The affected product anchors PKI and certificate lifecycle infrastructure, meaning a successful compromise can undermine trust across the entire certificate chain an organization relies on. Vendor patches are available for all affected version branches; no workarounds exist, and patching is the required remediation path.

Technical Analysis

CVE-2026-0240 (CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere) affects Palo Alto Networks Trust Protection Foundation versions 24.1.0-24.1.12, 24.3.0-24.3.5, 25.1.0-25.1.7, and 25.3.0-25.3.2. An authenticated attacker positioned on an adjacent network can extract sensitive credentials from the product vault. Successful exploitation results in full user impersonation (MITRE T1078: Valid Accounts) and unrestricted configuration modification (T1565.001: Stored Data Manipulation). Additional relevant technique mappings include T1555 (Credentials from Password Stores), T1552 (Unsecured Credentials), T1552.001 (Credentials in Files), and T1552.004 (Private Keys). The vendor-reported CVSS base score is 5.0 (Medium); however, given the product's role as a PKI and certificate lifecycle trust anchor, operational severity in high-value environments may exceed this rating. Official NVD scoring is pending. No CISA KEV listing at time of

writing. Patches are available from Palo Alto Networks PSIRT across all affected branches.

Action Checklist

1. Step 1: Containment, Identify all Trust Protection Foundation instances running versions 24.1.0-24.1.12, 24.3.0-24.3.5, 25.1.0-25.1.7, or 25.3.0-25.3.2. Restrict adjacent-network access to the vault interface immediately using network segmentation or ACLs while patching is staged. Do not rely on access restrictions as a permanent fix; no workaround substitutes for the patch.
2. Step 2: Detection, Review authentication logs on Trust Protection Foundation instances for unexpected credential access events, vault read operations by non-standard accounts, or authenticated sessions from unexpected source IPs on adjacent network segments. Correlate against MITRE T1555 and T1552 detection use cases in your SIEM. Check for anomalous certificate issuance or PKI configuration changes that may indicate post-exploitation activity.
3. Step 3: Eradication, Apply vendor-issued patches from the Palo Alto Networks PSIRT advisory for your specific version branch (24.1.x, 24.3.x, 25.1.x, or 25.3.x). Consult the official Palo Alto Networks PSIRT advisory for your version branch; patch URLs and instructions are provided there. Verify patch integrity against vendor-published checksums before deployment.
4. Step 4: Recovery, After patching, rotate all credentials and private keys stored in or accessible through the Trust Protection Foundation vault. Audit PKI configuration for unauthorized changes introduced during any potential exploitation window. Verify certificate chain integrity across dependent systems. Monitor for anomalous certificate issuance for at least 30 days post-remediation.
5. Step 5: Post-Incident, Assess whether vault credential access is sufficiently logged for forensic purposes; if not, implement vault audit logging as a standing control. Review network segmentation controls isolating PKI infrastructure from adjacent-network attack surfaces. Map credential exposure from sensitive system stores to CIS Control 4 (Secure Configuration) and CIS Control 12 (Network Infrastructure Management) for gap remediation. Consider whether privileged vault credentials require additional protection under your PAM policy.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and initiate formal incident declaration if vault audit logs confirm any credential read or export operations by non-standard accounts during the exposure window, if any unauthorized certificates were issued by CAs managed through Trust Protection Foundation, or if the organization operates in a regulated industry (PCI-DSS, HIPAA, FedRAMP) where PKI compromise triggers breach notification obligations — a compromised certificate infrastructure affects trust across all dependent systems and may constitute a reportable incident even at CVSS 5.0.

Recovery Notes	After patching and credential rotation, verify PKI chain integrity by running 'certutil -verify -urlfetch ' against all certificates issued by CAs anchored to Trust Protection Foundation to confirm no rogue certificates remain trusted. Monitor Trust Protection Foundation vault access logs and CA issuance Event IDs 4886 and 4887 daily for a minimum of 30 days post-remediation, specifically watching for credential access by service accounts whose passwords were rotated, which may indicate an attacker persisted extracted credentials in an external tool. If any unauthorized certificate issuance is confirmed, treat this as an active compromise, expand the scope to all systems that trusted those certificates, and consider a full PKI re-key depending on the certificate hierarchy depth affected.
Forensic Artifacts	Trust Protection Foundation vault audit logs: Record credential read, export, and access operations by authenticated users — the primary artifact proving CVE-2026-0240 exploitation, as the vulnerability specifically enables extraction of vault-stored credentials by an authenticated adjacent-network attacker. | Windows Certification Authority event log (Microsoft-Windows-CertificationAuthority): Event IDs 4886 (certificate requested) and 4887 (certificate issued) during the exploitation window reveal whether extracted credentials were used for impersonation to request or issue unauthorized certificates. | Trust Protection Foundation application authentication logs: Session records showing source IPs, authenticated usernames, and timestamps of vault interface logins — identifies which adjacent-network hosts initiated sessions and whether non-standard accounts accessed the vault. | Network flow or packet capture data scoped to the vault interface port from adjacent network segments: Establishes a timeline of which hosts communicated with the Trust Protection Foundation vault interface, corroborating or refuting attacker adjacency claims and identifying potential pivot hosts. | PKI configuration export (pre- and post-exploitation): A diff of the Trust Protection Foundation configuration state before and after the exploitation window reveals unauthorized CA parameter changes, template modifications, or permission escalations consistent with post-exploitation configuration modification described in the CVE summary.

Per-Action IR Details

Step 1: Containment — Identify all Trust Protection Foundation instances running versions 24.1.0–24.1.12, 24.3.0–24.3.5, 25.1.0–25.1.7, or 25.3.0–25.3.2. Restrict adjacent-network access to the vault interface immediately using network segmentation or ACLs while patching is staged. Do not rely on access restrictions as a permanent fix — no workaround substitutes for the patch.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), 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) — implied by network segmentation requirement, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Use 'netstat -an | findstr LISTENING' (Windows) or 'ss -tlnp' (Linux) on each candidate host to confirm Trust Protection Foundation vault port exposure, then apply host-based Windows Firewall rules via 'netsh advfirewall firewall add rule name=TPF-VAULT-BLOCK dir=in action=block remoteip=' or iptables 'iptables -I INPUT -s -p tcp --dport -j DROP' to restrict adjacent-network reach immediately. Enumerate affected instances by querying your asset inventory or running an nmap service-version scan ('nmap -sV -p ') scoped to adjacent segments.

Evidence: Before implementing ACLs, capture current network connection state on each Trust Protection Foundation host using 'netstat -anob' (Windows) or 'ss -tlnp' plus 'lsof -i' (Linux) to establish a baseline of who held active vault sessions at time of containment. Export existing firewall rule tables ('netsh advfirewall export' or 'iptables-save') to document the pre-containment network exposure. Snapshot the Trust Protection Foundation vault access log directory (typically under the product's data or log path) to preserve pre-containment read/write events before log rotation can overwrite them.

Step 2: Detection — Review authentication logs on Trust Protection Foundation instances for unexpected credential access events, vault read operations by non-standard accounts, or authenticated sessions from unexpected source IPs on adjacent network segments. Correlate against MITRE T1555 and T1552 detection use cases in your SIEM. Check for anomalous certificate issuance or PKI configuration changes that may indicate post-exploitation activity.

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), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, parse Trust Protection Foundation application logs directly using PowerShell: 'Select-String -Path "C:*.log" -Pattern "vault|credential|read|export" | Select-Object LineNumber,Line | Export-Csv tpf_vault_hits.csv'. For PKI configuration changes, query the Windows Certificate Authority event log ('Get-WinEvent -LogName "Microsoft-Windows-CertificationAuthority"') filtering on Event IDs 4870 (certificate revoked), 4882 (CA permissions changed), and 4896 (rows deleted from certificate database). Use Wireshark or tcpdump with a capture filter scoped to the vault port ('tcp port and net ') to identify source IPs that communicated with the vault before containment. Map findings manually to MITRE T1555.004 (Credentials from Password Stores — Windows Credential Manager) and T1552.004 (Unsecured Credentials — Private Keys).

Evidence: Collect Trust Protection Foundation vault audit logs that record credential read and export operations — these are the primary artifact for T1555/T1552 exploitation of CVE-2026-0240, as the vulnerability enables an authenticated adjacent-network attacker to extract vault-stored credentials. Capture authentication logs showing session source IPs and timestamps for vault interface logins, particularly any accounts that do not match the expected service account baseline. Export the PKI Certificate Authority database query history and any issuance events (Windows CA: Event ID 4886 — Certificate requested, Event ID 4887 — Certificate issued) that occurred in the exploitation window, as post-exploitation impersonation would likely drive unauthorized certificate requests.

Step 3: Eradication — Apply vendor-issued patches from the Palo Alto Networks PSIRT advisory (https://security.paloaltonetworks.com/CVE-2026-0240) for your specific version branch: 24.1.x, 24.3.x, 25.1.x, or 25.3.x. Verify patch integrity against vendor-published checksums before deployment.

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), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Verify patch file integrity before deployment by computing the SHA-256 hash of the downloaded installer and comparing it to the checksum published in the Palo Alto PSIRT advisory: 'Get-FileHash -Algorithm SHA256 .\' (Windows) or 'sha256sum ' (Linux). If automated patching is unavailable, follow the manual upgrade path documented in the Palo Alto Trust Protection Foundation upgrade guide for your specific version branch (24.1.x, 24.3.x, 25.1.x, 25.3.x) and take a VM snapshot or filesystem backup immediately before applying the patch to enable rollback. Document the pre- and post-patch version string from the application's version endpoint or 'about' page as evidence of successful remediation.

Evidence: Before patching, capture a full filesystem listing of the Trust Protection Foundation installation directory ('Get-ChildItem -Recurse | Select FullName,LastWriteTime,Length' or 'find /opt/ -type f -ls') to establish a pre-patch baseline for post-patch integrity comparison. Preserve a copy of the running Trust Protection Foundation configuration export, as this documents the vault state at time of eradication and provides a reference if unauthorized configuration changes are discovered during the recovery phase. Note the exact installed version string ('Get-WmiObject Win32_Product | Where-Object {$_.Name -like '*Trust Protection*'}' or equivalent) as forensic evidence of the vulnerable version that was running prior to remediation.

Step 4: Recovery — After patching, rotate all credentials and private keys stored in or accessible through the Trust Protection Foundation vault. Audit PKI configuration for unauthorized changes introduced during any potential exploitation window. Verify certificate chain integrity across dependent systems. Monitor for

anomalous certificate issuance for at least 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST SC-17 (Public Key Infrastructure Certificates), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Enumerate all certificates issued by CAs managed through Trust Protection Foundation during the exploitation window using the Windows CA cmdlet 'certutil -view -out "RequestID,RequesterName,NotBefore,NotAfter,CertificateTemplate" -restrict "NotBefore>="' and flag any certificates issued to unexpected requesters or using privileged templates. For private key rotation without enterprise PAM tooling, use 'certutil -repairstore' to verify key store integrity and manually revoke suspect certificates via the CA MMC console (Certification Authority → Issued Certificates → right-click → Revoke). Publish a CRL update immediately after revocation ('certutil -crl') and verify dependent systems are consuming the updated CRL.

Evidence: Capture a full export of the Trust Protection Foundation vault contents (credential inventory, certificate objects, and private key references) post-patch as an authoritative baseline to compare against the pre-exploitation state. Pull the CA issuance log covering the exploitation window and flag any certificate requests (Event ID 4886) and issuances (Event ID 4887) that do not match approved requesters or templates — these would represent the direct impact of attacker impersonation using vault-extracted credentials. Document the serial numbers and subjects of all certificates that must be revoked as forensic evidence of post-exploitation activity scope.

Step 5: Post-Incident — Assess whether vault credential access is sufficiently logged for forensic purposes; if not, implement vault audit logging as a standing control. Review network segmentation controls isolating PKI infrastructure from adjacent-network attack surfaces. Map this vulnerability pattern to CIS Control 4 (Secure Configuration) and CIS Control 12 (Network Infrastructure Management) for gap remediation. Consider whether privileged vault credentials require additional protection under your PAM policy.

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 AU-2 (Event Logging), NIST AU-9 (Protection of Audit Information), NIST AU-11 (Audit Record Retention), NIST RA-3 (Risk Assessment), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: For vault audit logging without a commercial PAM solution, enable Trust Protection Foundation's native audit logging at maximum verbosity per the Palo Alto product documentation and forward log output to a dedicated syslog collector (syslog-ng or rsyslog) on a hardened host outside the PKI segment to prevent log tampering. Write a Sigma rule targeting vault credential-read patterns in the Trust Protection Foundation log format and validate it against the log samples captured during this incident to ensure future detections fire correctly. For network segmentation verification, run an nmap scan from an adjacent-segment host post-remediation ('nmap -sV -p ') to confirm the vault interface is no longer reachable from adjacent networks.

Evidence: Compile the complete incident timeline artifact set: vault access logs covering the exposure window, CA issuance events, network connection logs showing adjacent-segment source IPs, and the pre/post-patch configuration exports. This package constitutes the forensic record for the CVE-2026-0240 exposure and must be retained per your organization's audit record retention policy (NIST AU-11) — minimum 1 year is recommended given the PKI trust chain implications. Document any certificates that were revoked and the dependent systems that consumed updated CRLs as evidence that the PKI trust chain was fully remediated.

Detection Guidance

Focus detection on the Trust Protection Foundation vault access layer. Query authentication and access logs for: (1) vault read operations by accounts outside expected service account baselines; (2) authenticated

sessions originating from unexpected hosts on adjacent network segments; (3) bulk or rapid-sequence credential retrieval events, which may indicate automated extraction. In your SIEM, build a detection aligned to MITRE T1555 (Credentials from Password Stores) and T1552.004 (Private Keys) targeting Trust Protection Foundation log sources. Post-exploitation indicators to hunt for: new certificate issuance events not tied to approved requests, PKI configuration modifications outside change-window periods, and lateral movement using newly valid service or admin accounts that correlate in time with vault access anomalies. No public IOCs are available for this vulnerability at time of writing. Escalation flag: if you identify evidence of active exploitation, treat as an active incident and engage your incident response process.

Framework Mappings

MITRE-ATTACK

- **T1555** — Credentials from Password Stores
- **T1552.004** — Private Keys
- **T1552.001** — Credentials In Files
- **T1552** — Unsecured Credentials
- **T1565.001** — Stored Data Manipulation
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-2** — Flaw Remediation
- **SC-13** — Cryptographic Protection

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

HIPAA-SECURITY

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

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1555	Credentials from Password Stores	Credential-Access
T1552.004	Private Keys	Credential-Access
T1552.001	Credentials In Files	Credential-Access
T1552	Unsecured Credentials	Credential-Access
T1565.001	Stored Data Manipulation	Impact
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Palo Alto Networks Security Advisories	https://security.paloaltonetworks.com/CVE-2026-0240	T3
CVE-2026-24040: jsPDF Information Disclosure Vulnerability	https://www.sentinelone.com/vulnerability-database/cve-2026-24040/	T3
CVE-2026-24040 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-24040	T1
Exploitation of 'Copy Fail' Linux Vulnerability Begins - SecurityWeek	https://www.securityweek.com/exploitation-of-copy-fail-linux-vulner...	T3
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-0240	T1

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