INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-21 19:03 UTC

Trend Micro Apex One - Trend Micro Apex One (On-Premise) Directory Traversal Vulnerability

CVE VULNERABILITY | HIGH | CVSS 7.8 | CISA KEV

SCC Item ID	SCC-CVE-2026-0209
Type	CVE Vulnerability
CVE ID	CVE-2026-34926
Severity	HIGH
CVSS Base Score	7.8
KEV Status	Yes — CISA Known Exploited Vulnerability (due: 2026-06-04)
Affected Products	Trend Micro Apex One (On-Premise)
Published	2026-05-21
Discovery Source	Cisa Kev

Executive Summary

A directory traversal vulnerability in Trend Micro Apex One (on-premise) allows a local, pre-authenticated attacker to modify a server-side key table and inject malicious code that propagates to all managed endpoints across the deployment. CISA has confirmed active exploitation and set a federal remediation deadline of June 4, 2026. Organizations running on-premise Apex One deployments face potential enterprise-wide endpoint compromise from a single point of attack.

Technical Analysis

CVE-2026-34926 is a CWE-22 (Path Traversal) vulnerability in Trend Micro Apex One on-premise. A pre-authenticated local attacker can traverse directory boundaries to write to a key table on the Apex One server. Malicious code injected into that table is subsequently distributed to all managed agents, enabling lateral propagation across the entire managed endpoint fleet. MITRE ATT&CK techniques involved: T1083 (File and Directory Discovery), T1554 (Compromise Client Software Binary), T1105 (Ingress Tool Transfer). CVSS base score: 7.8 (High). CISA added this to the Known Exploited Vulnerabilities catalog with a federal agency remediation due date of 2026-06-04. No CVSS vendor score or EPSS data is currently populated in available sources. Patch and affected version details should be confirmed against the Trend Micro advisory. Primary sources (NVD, CISA KEV) are authoritative; vendor advisory details should be confirmed directly with Trend Micro before operational decisions.

Action Checklist

1. Step 1: Containment, Immediately isolate the Apex One on-premise server from untrusted network segments. Restrict local logon access to the Apex One server to named administrators only, enforcing least privilege (NIST AC-6, CIS 5.4). Do not allow general user sessions on the Apex One management host until patched.
2. Step 2: Detection, Review Apex One server logs for unauthorized file writes or modification events targeting key table files. Hunt for anomalous agent policy pushes or unexpected binary deployments to managed endpoints (T1105, T1554). Query endpoint EDR telemetry for new or modified executables deployed via the Apex One agent update mechanism from an unexpected baseline. No specific IOCs are confirmed in current source data; monitor for behavioral indicators until vendor IOC guidance is published.
3. Step 3: Eradication, Apply the Trend Micro patch referenced in the Apex One security bulletin. Verify the patch version against Trend Micro's official advisory; confirm the exact build number directly with Trend Micro before declaring remediation complete. After patching, audit the key table for unauthorized modifications and rebuild from a known-good baseline if tampering is detected.
4. Step 4: Recovery, After patching, conduct a full integrity check of all managed agent binaries across the endpoint fleet using host-based file integrity monitoring (HBFIM) and cryptographic hash verification. Verify no unauthorized code was distributed to agents prior to remediation. Re-establish a clean configuration baseline (CIS 4.6). Monitor agent update traffic for anomalies for at least 14 days post-patch.
5. Step 5: Post-Incident, This vulnerability exposed a gap in local access controls on the Apex One server and agent update trust. Review whether the Apex One server meets NIST CM-6 hardening requirements. Evaluate agent update signing and verification controls. Implement credential rotation for any accounts with local access to the Apex One server (NIST AC-2). Document findings per NIST IR-4 and update the vulnerability management process to include security tool servers as priority patching targets.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if any managed endpoint hash comparison reveals confirmed distribution of malicious binaries prior to patching, as this constitutes potential enterprise-wide compromise with regulatory breach notification obligations under applicable data protection frameworks (e.g., HIPAA, PCI DSS, state breach notification laws) given the blast radius of the Apex One agent update mechanism.
Recovery Notes	Recovery cannot be declared complete until SHA-256 hash verification of Apex One agent binaries has been completed across 100% of managed endpoints — not just a sample — given the exploit's ability to propagate malicious code to every agent in the deployment from a single server-side key table modification. Post-patch monitoring of Apex One agent-to-server update traffic should continue for a minimum of 14 days using network traffic baselines established from a clean post-patch reference capture, watching for update package size anomalies or unexpected update frequencies that could indicate persistence mechanisms surviving the patch. Re-establish and formally document the Apex One server configuration baseline under NIST CM-2 (Baseline Configuration) immediately after recovery to ensure any future deviation is detectable.

Forensic Artifacts	Apex One server key table files under `%OFFICESCAN_HOME%\PCCSRV\` — directory traversal exploitation of CVE-2026-34926 would produce unauthorized writes or modifications to these files with timestamps falling outside normal Trend Micro update cycles; hash and timestamp these files immediately upon isolation. | Windows Security Event Log Event ID 4663 (An attempt was made to access an object) on the Apex One server filtered to the key table directory path — this event will capture the file write operations performed by the local pre-authenticated attacker exploiting the directory traversal vulnerability. | Apex One server-side policy propagation and agent update logs at `%OFFICESCAN_HOME%\PCCSRV\Log\TMNotify.log` and `update.log` — these will show the timestamp and scope of any malicious binary or policy push distributed to managed endpoints following key table compromise. | SHA-256 hashes of Apex One agent executables (`ntrtscan.exe`, `pccntmon.exe`, `TmListen.exe`, and associated DLLs) collected from all managed endpoints via PowerShell remoting — binaries modified after the key table compromise timestamp and before patching represent confirmed payload distribution artifacts specific to this attack chain. | Windows Registry key `HKLM\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion` on managed endpoints — unauthorized configuration values injected via the compromised key table propagation mechanism would appear here, and comparison across the fleet against a known-good baseline will scope the full extent of endpoint tampering.

Per-Action IR Details

Step 1: Containment — Immediately isolate the Apex One on-premise server from untrusted network segments. Restrict local logon access to the Apex One server to named administrators only, enforcing NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts). Do not allow general user sessions on the Apex One management host until patched.

NIST Phase: Containment

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

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: On the Apex One server host, run: `net localgroup administrators` to enumerate all accounts with local admin rights and remove non-essential entries. Use Windows Firewall via `netsh advfirewall firewall add rule name='Apex One Isolation' dir=in action=block remoteip=any` with explicit ALLOW rules for only named admin workstations by IP. Disable interactive logon for service accounts via Local Security Policy (secpol.msc) → Local Policies → User Rights Assignment → 'Deny log on locally'. A 2-person team can complete firewall ACL enforcement and account audit within 30 minutes.

Evidence: Before restricting access, capture a full snapshot of: (1) current local group membership via `net localgroup administrators > localadmins_baseline.txt`; (2) active sessions on the Apex One server via `query session` and `qwinsta`; (3) Windows Security Event Log Event ID 4624 (Successful Logon) and 4625 (Failed Logon) filtered to the Apex One server for the prior 72 hours to identify any pre-exploitation local access; (4) current network connections from the Apex One server via `netstat -anob > netstat_baseline.txt` to identify any unexpected outbound C2 channels established post-exploitation; (5) Apex One server-side audit logs at `%OFFICESCAN_HOME%\PCCSRV\Log\` for session records prior to isolation.

Step 2: Detection — Review Apex One server logs for unauthorized file writes or modification events targeting key table files. Hunt for anomalous agent policy pushes or unexpected binary deployments to managed endpoints (T1105, T1554). Query endpoint EDR telemetry for new or modified executables deployed via the Apex One agent update mechanism from an unexpected baseline. Correlate with NIST AU-6 (Audit Record Review) and CIS 8.2 (Collect Audit Logs). No specific IOCs are confirmed in current source data — monitor for behavioral indicators until vendor IOC guidance is published.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without EDR: (1) Deploy Sysmon with SwiftOnSecurity config on the Apex One server and all managed endpoints — focus on Event ID 11 (FileCreate) and Event ID 1 (ProcessCreate) filtering on the Apex One agent installation directory (default: `C:\Program Files (x86)\Trend Micro\OfficeScan Client\`). (2) Run this PowerShell on the Apex One server to detect recent key table modifications: `Get-ChildItem -Path 'C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV\' -Recurse -File | Where-Object { $_.LastWriteTime -gt (Get-Date).AddDays(-7) } | Select-Object FullName, LastWriteTime, Length | Export-Csv keytable_changes.csv`. (3) Use Sigma rule for T1554 (Compromise Client Software Binary) adapted to monitor Apex One agent binary paths. (4) On endpoints, compare SHA-256 hashes of agent binaries against a known-good baseline using `Get-FileHash 'C:\Program Files (x86)\Trend Micro\OfficeScan Client\*.exe' -Algorithm SHA256`.

Evidence: Before log review, preserve: (1) Apex One server-side component update logs at `%OFFICESCAN_HOME%\PCCSRV\Log\ofcserver.ini` and `update.log` for anomalous update package creation timestamps; (2) Windows Security Event Log Event ID 4663 (Object Access — file write) on the Apex One server targeting the key table directory path; (3) Apex One agent deployment/policy push logs at `%OFFICESCAN_HOME%\PCCSRV\Log\` — specifically `TMNotify.log` and `PolicyServer.log` for unexpected policy propagation events outside normal change windows; (4) Sysmon Event ID 1 (ProcessCreate) on managed endpoints showing processes spawned by the Apex One agent (`ntrtscan.exe`, `pccntmon.exe`) that fork unexpected child processes; (5) Network captures (Wireshark/tcpdump) on the port used for Apex One agent-server communication (default TCP 8080/10319) for unexpected binary payloads in update traffic.

Step 3: Eradication — Apply the Trend Micro patch referenced in the Apex One security bulletin (success.trendmicro.com/en-US/solution/KA-0023430). Verify the patch version against Trend Micro's official advisory — affected version specifics are not fully populated in current source data, so confirm the exact build number directly with Trend Micro before declaring remediation complete. After patching, audit the key table for unauthorized modifications and rebuild from a known-good baseline if tampering is detected.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For teams without automated patch orchestration: (1) Download the Trend Micro Apex One patch directly from the vendor portal after authenticating — do not use cached or third-party mirrors. (2) Verify the installer SHA-256 against Trend Micro's advisory before executing. (3) After patching, use PowerShell to audit key table file integrity: `Get-FileHash -Path 'C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV\\*' -Algorithm SHA256 | Export-Csv post_patch_keytable_hashes.csv` and compare against pre-patch hashes captured during evidence collection. (4) If tampering is confirmed, restore the key table from the most recent pre-compromise backup and re-validate hashes before re-enabling agent communication. Document exact patch build number, install timestamp, and validation outcome in the incident ticket.

Evidence: Before applying the patch, preserve: (1) Full forensic image or at minimum a volume shadow copy of the Apex One server disk to preserve pre-patch state for later forensic analysis; (2) Export all current Apex One key table files from `%OFFICESCAN_HOME%\PCCSRV\` with timestamps and hashes to establish the tampered baseline; (3) Windows Application and System Event Logs from the Apex One server covering the full suspected compromise window (minimum 30 days given active exploitation status); (4) A directory listing with hashes of all files under the Apex One installation directory: `Get-ChildItem -Recurse 'C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV\' | Get-FileHash -Algorithm SHA256 | Export-Csv pre_patch_full_inventory.csv`; (5) Running process list and loaded DLLs on the Apex One server via `Get-Process | Select-Object Name, Id, Path | Export-Csv pre_patch_processes.csv` to detect any injected or persistent malicious modules loaded into Apex One server processes.

Step 4: Recovery — After patching, conduct a full integrity check of all managed agent binaries across the endpoint fleet using D3-SFA (System File Analysis) and D3-FMBV (File Magic Byte Verification). Verify no unauthorized code was distributed to agents prior to remediation. Re-establish a clean configuration baseline per CIS 4.6 (Securely Manage Enterprise Assets and Software). Monitor agent update traffic for anomalies for at least 14 days post-patch.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-6 (Configuration Settings), NIST CM-2 (Baseline Configuration), NIST CP-10 (System Recovery and Reconstitution), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: For enterprise-scale agent verification without EDR: (1) Deploy a PowerShell remoting job across all managed endpoints to hash Apex One agent binaries: `Invoke-Command -ComputerName (Get-Content endpoints.txt) -ScriptBlock { Get-FileHash -Path 'C:\Program Files (x86)\Trend Micro\OfficeScan Client\*.exe' -Algorithm SHA256 } | Export-Csv agent_hash_audit.csv`. Compare output against a known-good hash baseline from a clean, unpatched-then-freshly-patched reference agent. (2) Use YARA rules targeting anomalous PE characteristics in the Apex One agent directory — specifically scanning for embedded shellcode or appended sections inconsistent with legitimate Trend Micro binaries. (3) Monitor Apex One agent-to-server TCP traffic on port 10319 (default) using Wireshark/tcpdump on the server NIC for 14 days, alerting on update packages with unexpected sizes or frequencies outside normal signature-update cycles.

Evidence: Before clearing endpoints for return to production: (1) Collect SHA-256 hashes of all Apex One agent executables and DLLs from every managed endpoint and compare against the post-patch clean baseline — discrepancies indicate pre-remediation malicious binary distribution; (2) Capture Windows Security Event Log Event ID 7045 (New Service Installed) and 4697 (Service Installed) on managed endpoints for the compromise window to detect malicious services installed via the Apex One agent update mechanism; (3) Review Prefetch files (`C:\Windows\Prefetch\`) on endpoints for execution of unexpected binaries timestamped to coincide with Apex One update events during the compromise window; (4) Check `HKLM\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion` registry hive on managed endpoints for unauthorized configuration changes pushed via the compromised key table; (5) Collect Apex One client-side logs from `C:\Program Files (x86)\Trend Micro\OfficeScan Client\ConnLog.log` on a representative sample of endpoints to identify any unexpected update payloads received.

Step 5: Post-Incident — This vulnerability exposed a gap in local access controls on the Apex One server and agent update trust. Review whether the Apex One server meets NIST CM-6 (Configuration Settings) hardening requirements. Evaluate agent update signing and verification controls. Implement D3-CRO (Credential Rotation) for any accounts with local access to the Apex One server. Document findings per NIST IR-4 (Incident Handling) and update the vulnerability management process per CIS 7.1 and 7.2 to include security tool servers as priority patching targets.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST CM-6 (Configuration Settings), NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.2 (Use Unique Passwords)

Compensating: For credential rotation without a PAM solution: (1) Use `net user ` for local accounts and `Set-ADAccountPassword` for domain accounts that had interactive access to the Apex One server. (2) Audit Apex One server service accounts via `sc qc ` for each Trend Micro service and rotate any shared or default credentials. (3) Document the hardening gap in a lessons-learned report mapping the CVE-2026-34926 directory traversal path to the specific missing control (agent update signing verification) and submit to vulnerability management as a recurring audit checklist item for all security tool servers. (4) Cross-reference the Apex One server against the CIS Benchmark for Windows Server applicable to the OS version and document any deviations as remediation backlog items.

Evidence: For the post-incident report, preserve and document: (1) The full key table audit trail showing pre-compromise, tampered, and restored states with file hashes and timestamps; (2) Timeline reconstruction from Apex One server logs correlating the first unauthorized key table write to the first anomalous agent policy push, establishing the exploitation-to-propagation interval; (3) Complete account access audit covering all local and domain accounts that authenticated to the Apex One server during the compromise window (Event IDs 4624, 4648, 4672); (4) Inventory of all managed endpoints that received agent updates during the compromise window, with hash comparison results, to scope the potential blast radius for board/executive reporting; (5) Lessons-learned documentation per NIST 800-61r3 §4 capturing: root cause (directory traversal in Apex One on-premise), detection gap (security tool servers excluded from priority patch SLAs), and corrective actions (agent update signing verification, server hardening baseline, privileged access restriction).

Detection Guidance

No confirmed IOCs (IPs, hashes, domains) are available in current source data for this CVE. Detection should focus on behavioral indicators. On the Apex One server: monitor file system audit logs for writes to key table directories outside of normal patch/update windows (NIST AU-2, AU-12; CIS 8.2). On managed endpoints: alert on unexpected binary deployments or executable modifications originating from the Apex One agent update channel (T1105, T1554). Cross-reference agent software inventory baselines (CIS 2.1) to identify introduced binaries. Use host-based file integrity monitoring (HBFIM) to monitor system file integrity on both the Apex One server and high-value managed endpoints. If a SIEM is in place, create a detection rule for Apex One server processes writing to key table paths at unexpected times or under unexpected user contexts. Flag any agent policy push that occurs outside a documented change window.

Framework Mappings

MITRE-ATTACK

- **T1083** — File and Directory Discovery
- **T1554** — Compromise Host Software Binary
- **T1105** — Ingress Tool Transfer

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-3** — Access Enforcement
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **16.12** — Implement Code-Level Security Checks

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

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
T1083	File and Directory Discovery	Discovery
T1554	Compromise Host Software Binary	Persistence
T1105	Ingress Tool Transfer	Command-And-Control

Sources

Source	URL	Tier
cisa_kev	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
CVE-2026-42926 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-42926	T1
CVE-2026-34926 - "Apex One Directory Traversal Vulnerability"	https://cvefeed.io/vuln/detail/CVE-2026-34926	T3
Standard Endpoint Protection (SEP) May 2026 Security Bulletin	https://success.trendmicro.com/en-US/solution/KA-0023430	T3
CVE-2026-21726 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2026-21726	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-34926	T1

Generated 2026-05-21 19:03 UTC by TJS Security Command Center