Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-34926: Trend Micro Apex One Under Active Exploitation

Date of Publication	Admiralty Code	TA Number
May 27, 2026	A1	TA2026148

Summary

First Seen: May 21, 2026
Targeted Platform: Windows
Affected Products: Trend Micro Apex One (On-Premise) 2019, Trend Micro Apex One as a Service, Trend Micro Vision One Endpoint Security - Standard Endpoint Protection (SEP)
Impact: Trend Micro disclosed CVE-2026-34926, a directory traversal vulnerability in the Apex One 2019 on-premise server that is being actively exploited in the wild. A pre-authenticated attacker with admin access to the Apex One server can modify a key table and inject malicious code that is then automatically distributed to all connected endpoint agents. Although rated Medium (CVSS 6.7), the flaw effectively turns the EDR's own update channel into a fleet-wide payload delivery mechanism, collapsing the trust boundary between the management server and protected endpoints. The same bulletin addresses seven additional local privilege escalation flaws in the Apex One/SEP agent. Organizations running Apex One 2019 on-prem must immediately upgrade to SP1 CP Build 18012 or SP1 Build 17079 with agent 14.0.0.17079.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-34926	Apex One Server Directory Traversal Vulnerability	Trend Micro Apex One (On-Premise)	✓	✓	✓
CVE-2026-34927	Security Agent Origin Validation Error Local Privilege Vulnerability	Trend Micro Apex One / Vision One SEP Agent	✗	✗	✓
CVE-2026-34928	Security Agent Origin Validation Error Local Privilege Vulnerability	Trend Micro Apex One / Vision One SEP Agent	✗	✗	✓
CVE-2026-34929	Security Agent Origin Validation Error Local Privilege Vulnerability	Trend Micro Apex One / Vision One SEP Agent	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-34930	Security Agent Origin Validation Error Local Privilege Vulnerability	Trend Micro Apex One / Vision One SEP Agent	✗	✗	✓
CVE-2026-45206	Security Agent Origin Validation Error Local Privilege Vulnerability	Trend Micro Apex One / Vision One SEP Agent	✗	✗	✓
CVE-2026-45207	Security Agent Origin Validation Error Local Privilege Vulnerability	Trend Micro Apex One / Vision One SEP Agent	✗	✗	✓
CVE-2026-45208	Security Agent Time-Of-Check Time-Of-Use Local Privilege Vulnerability	Trend Micro Apex One / Vision One SEP Agent	✗	✗	✓

Vulnerability Details

#1

CVE-2026-34926 is a relative path traversal vulnerability (CWE-23) in the on-premise server component of Trend Micro Apex One 2019, an enterprise endpoint detection and response platform deployed to manage and protect large fleets of Windows endpoints. The flaw was disclosed on May 21, 2026 under Trend Micro bulletin KA-0023430 and carries a CVSSv3.1 score of 6.7 (Medium); despite the medium rating, the flaw has been exploited in the wild. The same bulletin also addresses seven additional local privilege escalation flaws (CVE-2026-34927 through 34930 and CVE-2026-45206 through 45208) in the Apex One/SEP agent.

#2

The vulnerability stems from improper sanitization of file paths when the Apex One management server accesses internal server directories. A pre-authenticated attacker with administrative credentials to the Apex One server, obtained through phishing, credential theft, or lateral movement from another compromised host, can traverse outside the intended directory scope and reach sensitive server-side data structures that should be isolated from user-controlled write operations.

#3 The exploitation primitive centers on modifying a key table stored on the server. Because this key table is parsed during routine server-to-agent communication, the attacker effectively turns a configuration data structure into a code-delivery channel. There is no need to drop binaries on disk, register persistence mechanisms, or trigger conventional malware detections, since the payload travels through legitimate management traffic that endpoints are configured to trust implicitly.

#4 The downstream impact is what elevates this beyond a typical medium-severity issue. Once the key table is poisoned, the Apex One server distributes the injected payload to every connected endpoint agent during its next sync cycle, weaponizing the EDR's own trusted update mechanism for fleet-wide payload delivery. This collapses the security tool's trust boundary, allowing an attacker who has compromised a single management server to achieve mass code execution on endpoints that explicitly trust the server.

#5 Trend Micro confirmed at least one in-the-wild exploitation attempt observed by its Incident Response team prior to disclosure, which is what prompted the out-of-band ITW bulletin rather than a routine quarterly advisory. Affected builds are Apex One 2019 on-prem server and agent versions below 17079; remediation requires SP1 CP Build 18012 or SP1 Build 17079 with agent 14.0.0.17079.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-34926	Trend Micro Apex One 2019 (On-Premise) - Server and Agent builds below 17079	cpe:2.3:a:trendmicro:apex_one:*:*:*:*:on-premises:windows:*:* cpe:2.3:a:trendmicro:apex_one:*:*:*:*:saas:windows:*:*	CWE-23

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-34927	Trend Micro Apex One 2019 (On-Premise) Agent below 17079; Apex One as a Service / Vision One SEP Agent below 14.0.20731	cpe:2.3:a:trendmicro:apex_one:*:*:*:*:on-premises:windows:*:* cpe:2.3:a:trendmicro:apex_one:*:*:*:*:saas:windows:*:*	CWE-346
CVE-2026-34928	Trend Micro Apex One 2019 (On-Premise) Agent below 17079; Apex One as a Service / Vision One SEP Agent below 14.0.20731	cpe:2.3:a:trendmicro:apex_one:*:*:*:*:on-premises:windows:*:* cpe:2.3:a:trendmicro:apex_one:*:*:*:*:saas:windows:*:*	CWE-346
CVE-2026-34929	Trend Micro Apex One 2019 (On-Premise) Agent below 17079; Apex One as a Service / Vision One SEP Agent below 14.0.20731	cpe:2.3:a:trendmicro:apex_one:*:*:*:*:on-premises:windows:*:* cpe:2.3:a:trendmicro:apex_one:*:*:*:*:saas:windows:*:*	CWE-346
CVE-2026-34930	Trend Micro Apex One 2019 (On-Premise) Agent below 17079; Apex One as a Service / Vision One SEP Agent below 14.0.20731	cpe:2.3:a:trendmicro:apex_one:*:*:*:*:on-premises:windows:*:* cpe:2.3:a:trendmicro:apex_one:*:*:*:*:saas:windows:*:*	CWE-346

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-45206	Trend Micro Apex One 2019 (On-Premise) Agent below 17079; Apex One as a Service / Vision One SEP Agent below 14.0.20731	cpe:2.3:a:trendmicro:apex_one:*:*:*:*:on-premises:windows:*:*	CWE-346
CVE-2026-45207	Trend Micro Apex One 2019 (On-Premise) Agent below 17079; Apex One as a Service / Vision One SEP Agent below 14.0.20731	cpe:2.3:a:trendmicro:apex_one:*:*:*:*:on-premises:windows:*:*	CWE-346
CVE-2026-45208	Trend Micro Apex One 2019 (On-Premise) Agent below 17079; Apex One as a Service / Vision One SEP Agent below 14.0.20731	cpe:2.3:a:trendmicro:apex_one:*:*:*:*:on-premises:windows:*:*	CWE-367

Recommendations

Apply Patches Without Delay: Update Apex One (On-Premise) deployments to SP1 CP Build 18012 for existing SP1 installations, or to SP1 Build 17079 for fresh installations, ensuring the agent build is at least 14.0.0.17079. For Apex One as a Service and Vision One Endpoint Security - Standard Endpoint Protection deployments, roll out Security Agent build 14.0.20731 across the entire managed fleet.

Restrict and Audit Apex One Server Administrative Access: Because CVE-2026-34926 requires prior administrative credentials to the Apex One server, immediately review the list of accounts with administrative access to the Apex One management console and underlying server, remove unnecessary accounts, enforce strong unique passwords with multi-factor authentication, and ensure that administrative access is reachable only from trusted management networks via VPN, bastion, or privileged access workstation. Rotate credentials for any account suspected of exposure and review session and authentication logs for anomalous administrator activity since at least April 2026.

Hunt for Indicators of Compromise on Apex One Servers and Managed Agents: Given confirmed in-the-wild exploitation of CVE-2026-34926 and the vulnerability's ability to weaponize the agent deployment channel, investigate Apex One server file systems and key tables for unexpected modifications, scrutinize agent deployment package histories, and search managed endpoints for unexpected binaries, scheduled tasks, services, or persistence artifacts that arrived through the Apex One agent push mechanism. Treat any unexplained changes in the agent deployment pipeline as a potential intrusion event and escalate to incident response.

Harden Endpoint Privilege Boundaries: Because the seven agent-side flaws all require initial low-privileged code execution before privilege escalation, reduce the attack surface available to an unauthenticated foothold by enforcing application allow-listing, removing local administrator rights from standard users, restricting script interpreter usage, and ensuring endpoint detection and response telemetry is being centrally collected and reviewed for execution of unfamiliar binaries and tampering with security agent processes.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1078: Valid Accounts	
	T1190: Exploit Public-Facing Application	
Execution	T1203: Exploitation for Client Execution	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
Lateral Movement	T1072: Software Deployment Tools	

Patch Link

https://success.trendmicro.com/en-US/solution/KA-0023430

References

https://success.trendmicro.com/en-US/solution/KA-0023430

https://www.broadcom.com/support/security-center/protection-bulletin/cve-2026-34926-trend-micro-apex-one-on-premise-directory-traversal-vulnerability

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

May 27, 2026 • 07:40 AM

More at www.hivepro.com