ITW SECURITY BULLETIN: Apex One and Vision One – Standard Endpoint Protection (SEP) May 2026 Security Bulletin

Product / Version includes:

Apex One as a Service 2019 , Apex One 2019 , Apex One as a Service All , Apex One All , TrendAI Vision One™ Endpoint Security - Standard Endpoint

Last updated: 2026/05/21 Solution ID: KA-0023430 Category:

Summary

Release Date: May 21, 2026
CVE Identifiers: CVE-2026-34926 through 34930 and CVE-2026-45206 through 45208
Platform: Windows
CVSS 3.1 Score(s): 6.7-7.8
Severity Rating(s): MEDIUM - HIGH

TrendAI has released updates to Apex One (on-premise), Apex One as a Service and Vision One - Standard Endpoint Protection (SEP) to resolve multiple vulnerabilities.

! ITW Notification: TrendAI has observed at least one instance of an attempt to actively exploit one of these vulnerabilities in the wild.

Affected Version(s)

Product	Affected Version(s)	Platform	Language(s)
Apex One	2019 (On-prem) Server and Agent builds below 17079	Windows	English
Apex One as a Service TrendAI Vision One Endpoint Security - Standard Endpoint Protection (SEP)	SaaS Agent builds below 14.0.20731	Windows	English

Solution

TrendAI has released the following solutions to address the issue:

Product	Updated version	Platform	Availability
Apex One (on-prem)	SP1 CP Build 18012 (for existing SP1 users)* OR SP1 Build 17079 (for new installs) at least agent build 14.0.0.17079	Windows	Now Available
Apex One as a Service TrendAI Vision One SEP	Security Agent build 14.0.20731	Windows	Now Available

** Please note: while the vulnerabilities were originally addressed in the CP 17079 build, the Critical Patch update for existing SP1 users was removed due to an unrelated issue and replaced with the CP*

18012 version. Customers who have already applied the previous CP 17079 build or installs a fresh 17079 build are already protected.

These are the minimum recommended version(s) of the patches and/or builds required to address the issue. TrendAI highly encourages customers to obtain the latest version of the product if there is a newer one available than the one listed in this bulletin.

Customers are encouraged to visit TrendAI's Download Center to obtain prerequisite software (such as Service Packs) and to apply any of the on-prem solutions above.

Vulnerability Details

CVE-2026-34926: **Apex One Server Directory Traversal Vulnerability**

CVSSv3.1: 6.7: AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:L

Weakness: CWE-23

A directory traversal vulnerability in the Apex One (on-premise) server could allow a pre-authenticated local attacker to modify a key table on the server to inject malicious code to deploy to agents on affected installations.

*This vulnerability **is only exploitable** on the on-premise version of Apex One and a potential attacker must have access to the Apex One Server and already obtained administrative credentials to the server via some other method to exploit this vulnerability.*

Please Note - TrendAI has observed at least one attempt to exploit this vulnerability in the wild (ITW)!

CVE-2026-34927: **Security Agent Origin Validation Error Local Privilege Vulnerability**

ZDI-CAN-27959

CVSSv3.1: 7.8: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Weakness: CWE-346

An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations.

Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

CVE-2026-34928: **Security Agent Origin Validation Error Local Privilege Vulnerability**

ZDI-CAN-28061

CVSSv3.1: 7.8: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Weakness: CWE-346

An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-34927 but exists in a different named pipe communication mechanism.

Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

CVE-2026-34929: **Security Agent Origin Validation Error Local Privilege Vulnerability**

ZDI-CAN-28077

CVSSv3.1: 7.8: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Weakness: CWE-346

An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-34927 but exists in a different inter-process communication mechanism.

Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

CVE-2026-34930: **Security Agent Origin Validation Error Local Privilege Vulnerability**

ZDI-CAN-28089

CVSSv3.1: 7.8: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Weakness: CWE-346

An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-34927 but exists in a different process protection mechanism.

Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

CVE-2026-45206: **Security Agent Origin Validation Error Local Privilege Vulnerability**

ZDI-CAN-28118

CVSSv3.1: 7.8: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Weakness: CWE-346

An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-45207 but exists in a different process protection communication mechanism.

Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

CVE-2026-45207: **Security Agent Origin Validation Error Local Privilege Vulnerability**

ZDI-CAN-29177

CVSSv3.1: 7.8: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Weakness: CWE-346

An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-45206 but exists in a different process protection communication mechanism.

Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

CVE-2026-45208: **Security Agent Time-Of-Check Time-Of-Use Local Privilege Vulnerability**

ZDI-CAN-27982

settings. **Learn more**

CVSSv3.1: 7.8: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Weakness: CWE-367

A time-of-check time-of-use vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations.

Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

Mitigating Factors

Exploiting these type of vulnerabilities generally require that an attacker has access (physical or remote) to a vulnerable machine. In addition to timely application of patches and updated solutions, customers are also advised to review remote access to critical systems and ensure policies and perimeter security is up-to-date.

However, even though an exploit may require several specific conditions to be met, TrendAI strongly encourages customers to update to the latest builds as soon as possible.

Acknowledgement

TrendAI would like to thank the following individuals for responsibly disclosing these issues and working with Trend Micro to help protect our customers:

- TrendAI Incident Response (IR) Team (CVE-2026-34926)
- Lays (@_L4ys) of TRAPA Security working with TrendAI Zero Day Initiative (CVE-2026-34927 through 34930 & CVE-2026-45206 through 45208)

External Reference(s)

The [illegible] Zero Day Initiative Published Advisories site:

- ZDI-CAN-27939
- ZDI-CAN-28061
- ZDI-CAN-28077
- ZDI-CAN-28089
- ZDI-CAN-28118
- ZDI-CAN-29177
- ZDI-CAN-27982

---

settings. **Learn more**

English

TrendAI

Feedback

Support & Help	Resources	Policies & Vulnerability	About Trend
FAQ	Automation Center	Support Policies	TrendAI™
Contact by Sales	Download Center	Legal Policies & Privacy	Home & Home Office Support
	Education Portal	Vulnerability Response	Partner Portal
	Online Help Center		TrendAI™ YouTube Channel
	Service Status		
	TrendConnect Mobile App		