SECURITY BULLETIN: Apex One and Apex One (Mac) - February 2026

Product / Version includes:

Apex One 2019 , Apex One (Mac) All , Apex One All

Last updated: 2026/02/24 Solution ID: KA-0022458 Category:

Summary

Release Date: February 24, 2026
CVE Identifiers: CVE-2025-71210 through 71217
Platform: Windows, Mac
CVSS 3.1 Score(s): 7.2 - 9.8
Severity Rating(s): High - Critical

TrendAI has released a Critical Patch (CP) for Trend Micro Apex One as well as informational updates for SaaS updates for Apex One (Mac) for several vulnerabilities.

Affected Version(s)

Product	Affected Version(s)	Platform	Language(s)
Apex One	2019 (On-prem)	Windows	English
Apex One as a Service Trend Vision One Endpoint - Standard Endpoint Protection	SaaS	Windows	English

Solution

Trend Micro has released the following solutions to address the issue:

Product	Updated version		Platform
Apex One	CP Build 14136		Windows
Apex One as a Service Trend Vision One Endpoint - Standard Endpoint Protection	Security Agent Build 14.0.20315		Windows

Although some of these vulnerabilities may have been addressed by earlier versions patches and/or builds, it is always recommended to update to the latest build available.

Customers are encouraged to visit TrendAI's Download Center to obtain prerequisite software (such as Service Packs) before applying any of the solutions above.

Vulnerability Details (Windows)

CVE-2025-71210: **Console Directory Traversal Remote Code Execution Vulnerability**

ZDI-CAN-28001

CVSSv3: 9.8: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Weakness: CWE-22

A vulnerability in the Trend Micro Apex One management console could allow a remote attacker to upload malicious code and execute commands on affected installations.

Please note: although this vulnerability carries a technical critical CVSS rating, this was reported via responsible disclosure via a researcher through the Zero Day Initiative. ***The SaaS versions of the product have already been mitigated and no customer action required.***

For this particular vulnerability, an attacker must have access to the Trend Micro Apex One Management Console, so customers that have their console's IP address exposed externally should consider mitigating factors such as source restrictions if not already applied.

CVE-2025-71211: **Console Directory Traversal Remote Code Execution Vulnerability**

ZDI-CAN-28002

CVSSv3: 9.8: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Weakness: CWE-22

A vulnerability in the Trend Micro Apex One management console could allow a remote attacker to upload malicious code and execute commands on affected installations. This vulnerability is similar in scope to CVE-2025-71210 but affects a different executable.

Please note: although this vulnerability carries a technical critical CVSS rating, this was reported via responsible disclosure via a researcher through the Zero Day Initiative. ***The SaaS versions of the product have already been mitigated and no customer action required.***

For this particular vulnerability, an attacker must have access to the Trend Micro Apex One Management Console, so customers that have their console's IP address exposed externally should consider mitigating factors such as source restrictions if not already applied.

CVE-2025-71212: **Scan Engine Link Following Local Privilege Escalation Vulnerability**

ZDI-CAN-24972

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

Weakness: CWE-59

A link following vulnerability in the Trend Micro Apex One scan engine 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-2025-71213: **Origin Validation Error Local Privilege Escalation Vulnerability**

ZDI-CAN-26771

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

Weakness: CWE-346

An origin validation error vulnerability in Trend Micro Apex One 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.

Additional Vulnerability Enhancements (Windows)

In addition to addressing the vulnerabilities above, enhancements in the Critical Patch (ZDI-CAN-27975 & ZDI-CAN-27976) were made to improve protection against previous vulnerabilities (CVE-2025-54987 & CVE-2025-54948) in Apex One.

Informational Vulnerability Details (mac)

The following information is provided as informational only for CVE references, as these were addressed already via ActiveUpdate/SaaS updates in mid to late 2025 (SaaS 2507 & 2005 Yearly Release).

CVE-2025-71214: **Agent iCore Service Origin Validation Error Local Privilege Escalation Vulnerability**

ZDI-CAN-26282

CVSSv3: 7.2: AV:L/AC:H/PR:L/UI:R/S:C/C:N/I:H/A:H

Weakness: CWE-346

An origin validation error vulnerability in the Trend Micro Apex One (mac) agent iCore service 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-2025-71215: **Agent iCore Service Signature Verification Time-of-Check Time-of-Use Local Privilege Escalation Vulnerability**

ZDI-CAN-26609

CVSSv3: 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 Trend Micro Apex One (mac) agent iCore service signature verification 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-2025-71216: **Agent Cache Mechanism Time-of-Check Time-of-Use Local Privilege Escalation Vulnerability**

ZDI-CAN-26605

CVSSv3:7.8: 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 Trend Micro Apex One (mac) agent cache mechanism 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-2025-71217: **Agent Self Protection Origin Validation Error Local Privilege Escalation Vulnerability**

ZDI-CAN-26594

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

Weakness: CWE-346

An origin validation error vulnerability in the Trend Micro Apex One (mac) agent self-protection mechanism 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, Trend Micro strongly encourages customers to update to the latest builds as soon as possible.

Acknowledgement

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

- Jacky Hsieh and Charles Yang @ CoreCloud Tech. working with TrendAI's Zero Day Initiative (CVE-2025-71212, CVE-2025-71213)
- Anonymous working with TrendAI's Zero Day Initiative (CVE-2025-71212)

settings. Learn more

- Lays (@_L4ys) of TRAPA Security working with TrendAI's Zero Day Initiative (CVE-2025-71213 through 71217)

External Reference(s)

The following advisories may be found at Trend Micro's Zero Day Initiative Published Advisories site:

- ZDI-CAN-28001
- ZDI-CAN-28002
- ZDI-CAN-24972
- ZDI-CAN-26771
- ZDI-CAN-26282
- ZDI-CAN-26609
- ZDI-CAN-26605
- ZDI-CAN-26594

Was this article helpful?

settings. **Learn more**

Online Help Center

Service Status

TrendConnect Mobile App