



# SECURITY BULLETIN: December 2024 for Trend Micro Apex One

## Product / Version includes:

Apex One as a ServiceAll , Apex OneAll

 Last updated: 2024/12/16     Solution ID: KA-0018217     Category:

## Summary

**Release Date:** December 16, 2024

**CVE Identifiers:** CVE-2024-52048, CVE-2024-52049, CVE-2024-52050, CVE-2024-55631, CVE-2024-55632, CVE-2024-55917

**Platform:** Windows

**CVSS 3.0 Score(s):** 7.8

**Weakness ID(s):** CWE-266 (x2), CWE-59, CWE-269 (x2), CWE-346

**Severity Rating(s):** HIGH

Trend Micro has released new builds for Trend Micro Apex One and Apex One as a Service that resolve multiple vulnerabilities.

## Affected Version(s)

Product	Affected Version(s)	Platform	Language(s)
Apex One	2019 (On-prem) Versions before build 13140	Windows	English
Apex One as a Service	Versions before 202412 (Agent version 14.0.14203)	Windows	English

# Solution

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

Product	Updated version	Notes	Platform	Availability
Apex One	<a href="#">SP1 build 13140</a>	<a href="#">Readme</a>	Windows	Now Available
Apex One as a Service	December 2024 Monthly Maintenance (202412)  Agent version 14.0.14203	<a href="#">Notes</a>	Windows	Now Available

These are the minimum recommended version(s) of the patches and/or builds required to address the issue. Trend Micro 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 Trend Micro's [Download Center](#) to obtain prerequisite software (such as Service Packs) before applying any of the solutions above.

## Vulnerability Details

### CVE-2024-52048: LogServer Link Following Local Privilege Escalation Vulnerability

ZDI-CAN-24675

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

Weakness: CWE-266: Incorrect Privilege Assignment

A LogServer link following vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. This vulnerability is similar to, but not identical to CVE-2024-52049.

*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-2024-52049: LogServer Link Following Local Privilege Escalation Vulnerability**

ZDI-CAN-24674

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

Weakness: CWE-266: Incorrect Privilege Assignment

A LogServer link following vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. This vulnerability is similar to, but not identical to CVE-2024-52048.

*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-2024-52050: LogServer Arbitrary File Creation Local Privilege Escalation Vulnerability**

ZDI-CAN-24609

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

Weakness: CWE-59: Improper Link Resolution Before File Access

A LogServer arbitrary file creation 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.*

## **CVE-2024-55631: Engine Link Following Local Privilege Escalation Vulnerability**

ZDI-CAN-23995

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

Weakness: CWE-269: Improper Privilege Management

An engine link following 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.*

## **CVE-2024-55632: Security Agent Link Following Local Privilege Escalation Vulnerability**

ZDI-CAN-24557

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

Weakness: CWE-269: Improper Privilege Management

A security agent link following 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.*

## **CVE-2024-55917: Origin Validation Error Local Privilege Escalation Vulnerability**

ZDI-CAN-24566

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

Weakness: CWE-346: Origin Validation Error

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.*

## **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:

- Amol Dosanjh of [Trend Micro's Zero Day Initiative](#) (CVE-2024-52048, CVE-2024-52049, CVE-2024-52050)
- Frederik Reiter and Jan-Luca Gruber, cirosec GmbH working with [Trend Micro's Zero Day Initiative](#) (CVE-2024-55631)
- Anonymous working with [Trend Micro's Zero Day Initiative](#) (CVE-2024-55632)
- Lays (@\_L4ys) of TRAPA Security working with [Trend Micro's Zero Day Initiative](#) (CVE-2024-55917)

## External Reference(s)

*The following advisories may be found at [Trend Micro's Zero Day Initiative Published Advisories](#) site:*

- ZDI-CAN-24675
- ZDI-CAN-24674
- ZDI-CAN-24609
- ZDI-CAN-23995
- ZDI-CAN-24557
- ZDI-CAN-24566



Was this article helpful?



English



Feedback

## Support & Help

FAQ

Contact by Sales

## Resources

Automation Center

Download Center

Education Portal

Online Help Center

Service Status

TrendConnect Mobile App

## Policies & Vulnerability

Support Policies

Legal Policies & Privacy

Vulnerability Response

## About Trend

Trend Micro

Home & Home Office Support

Partner Portal

Trend Micro YouTube Channel

Copyright © 2025 Trend Micro Incorporated. All rights reserved.