[サポートニュース]アラート/アドバイザリ：TrendAI™ Apex Oneなどで確認された複数の脆弱性について(2026年5月)：TrendAI™ Apex One、Trend Micro Apex One as a Service、TrendAI Vision One™ Endpoint Security - Standard Endpoint Protection

製品・バージョン:

TrendAI Vision One™ All , Apex One as a Service All , Apex One All

更新日: 2026/05/21 記事ID: KA-0022974 カテゴリ:

概要

[公開日時：2026年05月21日 (木) 午前11時00分]

TrendAI™ Apex One (以下、Apex One) 、Trend Micro Apex One as a Service(以下、Apex One SaaS) 、TrendAI Vision One™ Endpoint Security - Standard Endpoint Protection (以下、Standard Endpoint Protection)において、複数の脆弱性（CVE-2026-34926 ～ CVE-2026-34930, CVE-2026-45206 ～ CVE-2026-45208）を確認しました。

トレンドマイクロは、これらの脆弱性のうちの1つ、CVE-2026-34926 が実際の攻撃に利用されたことを確認しています。

詳細は以下の通りです。

脆弱性の影響を受ける製品/コンポーネント/ツール

該当する脆弱性	製品/コンポーネント/ツール	CVSS3.0スコア	深刻度
CVE-2026-34926	Apex One Apex One SaaS Standard Endpoint Protection	6.7	中
CVE-2025-34927		7.8	高
CVE-2025-34928		7.8	高
CVE-2025-34929		7.8	高
CVE-2025-34930		7.8	高
CVE-2026-45206		7.8	高
CVE-2026-45207		7.8	高
CVE-2026-45208		7.8	高

脆弱性の概要

CVE-2026-34926: Apex One サーバにおけるディレクトリトラバーサルの脆弱性

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

Weakness: CWE-23

Apex One サーバーにおいて、ディレクトリトラバーサル脆弱性が確認されました。この脆弱性を悪用することで、ローカルの攻撃者はサーバー上の重要なテーブルを変更して、悪意のあるコードをエージェントに配布することができる可能性があります。

この脆弱性はオンプレミス版のApex Oneでのみ悪用可能です。攻撃者がこの脆弱性を悪用するためには、Apex Oneサーバーのいずれかの管理者資格情報を何らかの方法で取得している必要があります。

注意：トレンドマイクロは、この脆弱性が実際の攻撃に利用されたことを確認しています。オンプレミス版のApex Oneに対しては、できるだけ早く下記の対処法にある対処方法を適用することを推奨しています。

CVE-2026-34927: セキュリティエージェントにおける権限昇格につながる送信元確認が不十分な脆弱性

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

Apex Oneおよび、Standard Endpoint Protectionのエージェントにおいて、送信元確認が不十分な脆弱性が確認されました。この脆弱性により、ローカルの攻撃者は権限の昇格を行うことができる可能性があります。

この脆弱性を悪用するには、対象のシステムで低い権限でコードを実行できる必要があります。

CVE-2026-34928: セキュリティエージェントにおける権限昇格につながる送信元確認が不十分な脆弱性

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

Apex Oneおよび、Standard Endpoint Protectionのエージェントにおいて、送信元確認が不十分な脆弱性が確認されました。この脆弱性により、ローカルの攻撃者は権限の昇格を行うことができる可能性があります。

この脆弱性は、 CVE-2026-34927 と類似していますが異なる名前付きパイプに存在します。この脆弱性を悪用するには、対象のシステムで低い権限でコードを実行できる必要があります。

CVE-2026-34929: セキュリティエージェントにおける権限昇格につながる送信元確認が不十分な脆弱性

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

Apex Oneおよび、Standard Endpoint Protectionのエージェントにおいて、送信元確認が不十分な脆弱性が確認されました。この脆弱性により、ローカルの攻撃者は権限の昇格を行うことができる

可能性があります。

この脆弱性は、 CVE-2026-34927 と類似していますが異なる名前付きパイプに存在します。この脆弱性を悪用するには、対象のシステムで低い権限でコードを実行できる必要があります。

CVE-2026-34930: セキュリティエージェントにおける権限昇格につながる送信元確認が不十分な脆弱性

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

Apex Oneおよび、Standard Endpoint Protectionのエージェントにおいて、送信元確認が不十分な脆弱性が確認されました。この脆弱性により、ローカルの攻撃者は権限の昇格を行うことができる可能性があります。

この脆弱性は、 CVE-2026-34927 と類似していますが異なる名前付きパイプに存在します。この脆弱性を悪用するには、対象のシステムで低い権限でコードを実行できる必要があります。

CVE-2026-45206: セキュリティエージェントにおける権限昇格につながる送信元確認が不十分な脆弱性

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

Apex Oneおよび、Standard Endpoint Protectionのエージェントにおいて、送信元確認が不十分な脆弱性が確認されました。この脆弱性により、ローカルの攻撃者は権限の昇格を行うことができる可能性があります。

この脆弱性は、 CVE-2026-34927 と類似していますが異なる名前付きパイプに存在します。この脆弱性を悪用するには、対象のシステムで低い権限でコードを実行できる必要があります。

CVE-2026-45207: セキュリティエージェントにおける権限昇格につながる送信元確認が不十分な脆弱性

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

Apex Oneおよび、Standard Endpoint Protectionのエージェントにおいて、送信元確認が不十分な

脆弱性が確認されました。この脆弱性により、ローカルの攻撃者は権限の昇格を行うことができる可能性があります。

この脆弱性は、CVE-2026-34927と類似していますが異なる名前付きパイプに存在します。この脆弱性を悪用するには、対象のシステムで低い権限でコードを実行できる必要があります。

CVE-2026-45208: セキュリティエージェントにおけるローカル権限昇格につながる Time-of-Check Time-of-Use の脆弱性

ZDI-CAN-27982

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

Weakness: CWE-367

Apex Oneおよび、Standard Endpoint Protectionのエージェントにおいて、Time-of-Check Time-of-Use（ToCToU）の脆弱性が確認されました。この脆弱性により、ローカルの攻撃者は権限の昇格を行うことができる可能性があります。

この脆弱性を悪用するには、対象のシステムで低い権限でコードを実行できる必要があります。

対処方法

製品/コンポーネント/ツール	バージョン	修正	関連リン
Apex One	2019	CP 18012 ※ (Agent build 14.0.0.18012)	Readm
Apex One SaaS Standard Endpoint Protection	-	2026年4月メンテナンスで対応済み (Agent Build 14.0.20731)	FAQ情報

「修正」に記載されている内容は、掲載された脆弱性の対応に必要となる公表時点でのバージョン、ビルド番号です。より新しいバージョン、ビルドが公開されている場合は、最新のものを適用してください。

弊社では、広く最新の脅威に対応するために、常に最新のバージョンの製品をご利用いただくこと

を推奨しています。古いバージョンをお使いのお客様は新しいバージョンへのアップグレードをご検討ください。

※ これらの脆弱性の修正は元々は CP17079において行われましたが、この Critical Patch は、パッチ適用が正常に行われないことがある問題が確認されたため公開が停止されております。
そのため、入手可能な Critical PatchとしてCP 18012をご案内しております。すでに CP17079を適用した環境、および Service Pack 1 2025 (ビルド 17079) 新規インストール版 が適用済みの環境はすでに本脆弱性について保護された状態になっております。
CP17079の公開停止に関する情報については、下記のFAQをご参照お願いいたします。
参考：
[サポートニュース][更新]Trend Micro Apex One 2019 Critical Patch (ビルド 17079) 公開のお知らせ

軽減要素

この種の脆弱性を悪用するには、一般的に攻撃者が脆弱な端末にアクセスできることが必要です。 信頼されたネットワークからのみアクセスを許可することで、本脆弱性が利用される可能性を軽減することができます。

トレンドマイクロは、お客様にできるだけ早く最新のビルドにアップデートすることを推奨いたします。

更新情報

日付	更新履歴
2026年05月21日(木) 午前11時00分	情報公開

この記事は役に立ちましたか？

日本語

サポート

法人カスタマーサービス & サポート

FAQ

お問い合わせ一覧

その他

Education Portal

Online Help Center

オートメーションセンター

サービスステータスポータル

ダウンロード

お役立ち情報

サポートポリシー

ご利用条件

製品の脆弱性情報

会社概要

TrendAI™

個人のお客様

パートナーポータル

TrendAI™のYouTubeチャンネル

TrendAI

フィードバック