トレンドマイクロ社製ウイルス対策ソフトの問題を悪用する攻撃を観測

中国地域サイバーセキュリティ連絡会会員様
中国地域のサイバーセキュリティ担当者様

中国地域サイバーセキュリティ連絡会　事務局の木坂です。

Apex One 及びウイルスバスターコーポレートエディション XG 等の
セキュリティ上の問題を悪用した事例に関する注意喚起について、
以下のとおり情報展開させていただきます。
－－－

Apex One 及びウイルスバスターコーポレートエディション XG 等のセキュリティ上の問題を悪用した事例あり。
未対応の場合はアップデート及び回避策の検討を。

Ⅰ. 概要
　トレンドマイクロ社製ウイルス対策ソフト「Apex One」、「Apex One SaaS」、「ウイルスバスター コーポレートエディション XG」
ならびに「ウイルスバスター ビジネスセキュリティ 」のセキュリティ上の問題を悪用した攻撃がトレンドマイクロ社にて
確認されており、同社より注意喚起が公開されています。
　悪用された場合、システム内に侵入され不正操作やマルウェア感染等に繋がる恐れがあります。

■ 対象製品とバージョン
　　Trend Micro Apex One (以下、Apex One) 2019 バージョン Build 9565 未満
　　Trend Micro Apex One SaaS (以下、Apex One SaaS) バージョン Build 202107 未満
　　ウイルスバスター コーポレートエディション（以下、ウイルスバスター Corp.) XG Service Pack 1 バージョン Build 6058 未満
　　ウイルスバスター ビジネスセキュリティ 10.0 Service Pack 1 バージョン Build

2329 未満

Ⅱ. 対策・回避策
　システムを運用されている担当者や委託先事業者の窓口の方に、下記関連トピックを共有頂き、
該当製品を利用利用しているか確認のうえ、アップデート対応を行ってください。

－－

【関連トピック】
　Apex One、ウイルスバスターコーポレートエディション XG 等に脆弱性。悪用する攻撃が観測されているため、
対策版が公開された脆弱性に対するアップデートの検討を。
　対策版が未公開の脆弱性については回避策の検討を。

Ⅰ. 概要
　トレンドマイクロ社製「Apex One」、「Apex One SaaS」、「ウイルスバスター コーポレートエディション XG」
ならびに「ウイルスバスター ビジネスセキュリティ 」には、OS にログイン可能な第三者によって権限昇格され、
操作が可能となる 4 件の脆弱性が公開されています。
　このうち 2 件（CVE-2021-36741、CVE-2021-36742）の脆弱性を組み合わせて悪用する攻撃が観測されています。

影響： OS にログイン可能な第三者によって権限なしにファイルをアップロードされるなど悪用されたり、
　　サービス運用妨害（DoS）が行われる等の不正が行われる恐れがあります。

■ 対象製品とバージョン
　Trend Micro Apex One（以下、Apex One）2019 バージョン Build 9565 未満
　Trend Micro Apex One SaaS（以下、Apex One SaaS）バージョン Build 202107 未満

ウイルスバスター コーポレートエディション（以下、ウイルスバスター Corp.）
XG Service Pack 1 バージョン Build 6058 未満
ウイルスバスター ビジネスセキュリティ 10.0 Service Pack 1 バージョン Build 2329 未満

■ CVE 番号及び脆弱性の概要（CVSS3.0 基本値）
・CVE-2021-32464 (7.8) 不適切なパーミッション割り当てによる権限昇格の脆弱性
・CVE-2021-32465 (7.5) 不適切なパーミッションの保存による認証バイパスの脆弱性
・CVE-2021-36741 (7.1) 任意ファイルをアップロードされる脆弱性(※)
・CVE-2021-36742 (7.8) ローカルでの権限昇格の脆弱性(※)

※ 脆弱性を悪用する攻撃が確認されています。

Ⅱ. 対策・回避策
ベンダより回避策と対策版が提供されています。(詳細は「Ⅲ. 参考情報①～④」をご確認ください)

[回避策]
CVE-2021-32464, CVE-2021-32465 を解消した Apex One の最新バージョンについては 2021 年 8 月上旬に
ベンダーより公開される予定のため、ベンダーから公表されている情報（Ⅲ. 参考情報②）を参照の上、
記載されている以下の軽減要素の実施を検討ください。

・信頼されたネットワークからのみアクセスを許可する。

[対策]
ベンダーから公表されている情報（Ⅲ. 参考情報①～③）を参照のうえ、最新のバージョンにアップデートしてください。
製品のバージョン、ビルド情報の確認方法については、参考情報④を参照ください。

Ⅲ. 参考情報

① 【注意喚起】弊社製品の脆弱性（CVE-2021-36741,CVE-2021-36742）を悪用した攻撃を確認したことによる
修正プログラム適用のお願い
https://appweb.trendmicro.com/SupportNews/NewsDetail.aspx?id=4219
② アラート/アドバイザリ：ウイルスバスター コーポレートエディション、Trend Micro Apex One と
Trend Micro Apex One SaaS の脆弱性について（2021 年 7 月）
https://success.trendmicro.com/jp/solution/000287796
③ Apex One 2019 の最新版へバージョンアップしてご使用いただくまでの流れ
https://success.trendmicro.com/jp/solution/1123037
④ ウイルスバスター コーポレートエディション の製品情報(ビルド、パターンバージョン、
アクティベーションコードなど)確認方法
https://success.trendmicro.com/jp/solution/1309027