SPPM

SPPM3.0でVBBSSをご利用のお客様へ

【Windows】【VBBSS】
ActiveUpdateサーバのコードサイニング証明書更新に伴う影響について

株式会社AXSEED

2025年8月29日

AXSEED

経緯

お客様各位

平素はSPPM3.0をご利用いただきまして誠にありがとうございます。

SPPM3.0のWindowsのデバイス管理において、
「VBBSS (ウイルスバスター ビジネスセキュリティ サービス)」Ver.6.7をご利用のお客様環境に対し、
VBBSSではActiveUpdateサーバ(以下AUサーバ)からウイルスパターンファイルや検索エンジン等を
ダウンロードする際、それらのコンポーネントの真正性を確認する際に製品内部で
Azureコードサイニング証明書 (ACS)を使用しております。

2022年8月29日以来、長期でWindows PCをインターネットに接続していない場合、
Windows PCをインターネットに接続し、有効期限を更新した新証明書に対応するための
修正プログラムを適用いただく必要があります。
また、VBBSS側で保持している証明書データベースの有効期限が 2025年9月24日となっているため、
2025年9月24日までにインターネットに接続し、修正プログラムの適用をお願いいたします。

対象

■対象

ACS対応が必要な Windows PCでVBBSS(Secure Antivirusを含む)をご利用中で、
2022年8月29日以来、長期でWindows PCをインターネットに接続していない、
かつ添付資料の条件を満たしていないお客様

ACS対応が必要な OS	デフォルトで ACSに対応済みの OS (ACSに対応済みの OSであっても ルート証明書の適用が必要)
Windows 10 2004, 20H2, 21H1 Windows 10 1909 Windows 10 1809 Windows 10 1507	Windows 11 Windows 10 22H2 Windows 10 21H2

■影響を受ける事象

ActiveUpdate サーバのコードサイニング証明書更新 (2022年8月29日にリリース済みの修正プログラムの適用)を2025年9月24日までに実施しなかった場合、最新のパターンファイルなどのダウンロードに失敗します。
よって、古い定義ファイルによって定義されたものしか検知・駆除できなくなります。

VBBSSの修正プログラム適用条件

VBBSSの修正プログラムを適用するには条件 1,2のどちらも満たす必要があります。
条件を満たさない場合、VBBSSのバージョンが「6.7.3122/14.2.3072」で停止されます。

条件1)Windows OS の ACS対応セキュリティパッチが適用されていること (Windows の最小バージョン要件)

条件2)以下のルート証明書が OS にインストールされていること
「Microsoft Identity Verification Root Certificate Authority 2020」
(「ルート証明書の自動更新プログラム」が有効であれば自動的に適用されます)

条件2)のMicrosoftページからの抜粋
信頼された署名によって署名されたモジュールを正しく検証するには、
コンピューターに "Microsoft Identity Verification Root Certificate Authority 2020" 証明機関 (CA) が
インストールされている必要があります。
既定では、コンピューターがインターネットに接続されている場合、ルート証明書は自動的にインストールされます。
[ルート証明書の自動更新] 設定が無効になっている場合、またはコンピューターがオフラインの場合は、
"信頼されたルート証明機関" の下にある "ローカル コンピューター" の証明書ストアに
このルート証明書をインストールする必要があります。
ここまで

VBBSSのバージョンアップ停止の理由

条件を満たさない場合、VBBSSの修正プログラムが適用されなくなり、バージョンが「 6.7.3122/14.2.3072」で停止されます。

【停止の理由】
・ACS がサポートされていない OSのため、条件を満たさない。
・Microsoft社の仕様変更により、VBBSSのバージョンアップに ACSのチェックが必須化されたため、
VBBSSのバージョンアップが成功するまで ACSのチェックが繰り返されるため、
これによりACSがサポートされていない OSの場合、VBBSSのバージョンアップを行うことができず、
クライアントPCに対して、高い負荷をかけるため。

VBBSSのバージョンが「 6.7.2177 / 14.2.2120」以降であれば対応済みとなりますので、特に問題ありません。

■バージョンの確認方法
VBBSSのWeb管理コンソールにログイン
https://licensingplatform.trendmicro.com/xLP/Default.aspx?T=z77cC
(SPPM3.0管理画面 > 設定 > 契約情報 > Windows/PCタブ にIDが記載されています)

セキュリティエージェント > 設定の歯車アイコン > エージェントのバージョンにチェックして列を表示 > 適用
VBBSSのバージョンが「 6.7.2177 / 14.2.2120」以降になっていることを確認

補足

■2025年9月24日までに修正プログラムの適用ができなかった場合
条件を満たしたWindowsに、最新のVBBSSをインストールしなおしてください。

■トレンドマイクロ社公式ページ
https://success.trendmicro.com/ja-JP/solution/KA-0016221

前回のお知らせ内容 (2023年2月)

【SPPM3.0】(Windows)VBBSS モジュールの署名に伴う事前のWindowsセキュリティパッチ適用のお願い

SPPM3.0のWindowsのデバイス管理において、
「VBBSS (ウイルスバスター ビジネスセキュリティ サービス)」Ver.6.7を
ご利用のお客様に向けて、2023年2月中旬より、トレンドマイクロ社によって
モジュールの署名が実施されます。

後述するOSをご利用のお客様は、ご利用のWindows のバージョンに応じて、
Microsoft Windows セキュリティパッチを”事前に”適用をお願いいたします。

■対象
下記のWindows OSでVBBSSをご利用のお客様

■影響を受けるOS
Windows 10 2004, 20H2, 21H1※
Windows 10 1909※
Windows 10 1809※
Windows 10 1507※

※これらのセキュリティパッチの大半は 2021年9月または10月に最初に導入され、
その後 Microsoft の毎月の累積更新プログラムに含まれております。
そのため、Microsoft セキュリティパッチを最新の状態にしているお客様は、
すでに該当のパッチを適用済みの場合があります。

■必要な作業(各OSの最小バージョン要件を満たしていない場合)
1. 上記のOSをご利用の環境にて、OSのバージョンをご確認ください。
以下製品Q&Aに記載した各OSの最小バージョン要件を満たしていない場合は、
2023年2月中旬以降にリリースするVBBSSのモジュールを適用する前に、
Windows セキュリティパッチを適用してください。

<製品Q&A>:
重要なお知らせ:2023年2月以降に公開されるトレンドマイクロのサーバおよび
エンドポイント製品、および関連モジュールに関する Windows の
最小バージョン要件について
https://success.trendmicro.com/jp/solution/000291910
※本製品Q&Aには本件に関連する重要事項を記載しておりますのでご一読ください。

2.「信頼されたルート証明機関」にルート証明書「Microsoft Identity Verification Root
Certificate Authority 2020 」が適用されているかどうかご確認ください。
「信頼されたルート証明書」の自動更新が無効またはエアギャップ環境または
ロックダウン環境の場合、以下 URL に記載されているルート証明書
「 Microsoft Identity Verification Root Certificate Authority 2020 」を適用してください。
https://www.microsoft.com/pkiops/docs/repository.htm

■必要な作業が行えなかった場合
2023年2月中旬以降にリリースされるVBBSSのモジュールを適用した後、
本来であればセキュリティエージェントが正常に動かなくなりますが、
これを防ぐため、トレンドマイクロ社にて下記の対策を行っております。
ただし、当該機能の副作用として、以下の事象が発生いたします。

【発生する事象】
(1)各OSの最小バージョン要件を満たしていない環境には、2023年2月中旬以降に配信する
VBBSSの修正プログラムがVBBSSエージェント側に適用されません。
※旧Buildの状態で動作し続けるため、ウイルスパターンファイルは更新され続けます。
そのため、セキュリティ対策機能は担保できます。ご安心ください。
※ウイルス検索エンジンは修正プログラム内に含まれていますので更新されません。
その結果、新たな脅威への検出力低下への懸念が今後発生する可能性があります。

(2)(1)の結果、ネットワークトラフィックが増加し、ネットワークトラフィックの帯域幅が
圧迫される可能性があります。
※1時間置きに、1台あたり3MB前後の場合が通信が発生する可能性があります

(3)各OSの最小バージョン要件を満たしていない環境には、2023年2月中旬以降に、
新たなPCへVBBSSエージェントを新規インストールできない可能性があります。

この度はご面倒をおかけし誠に申し訳ございません。
その他、ご不明な点などがございましたら弊社サポート窓口までお問合せ下さい。
今後ともSPPM3.0をよろしくお願いいたします。


AXSEED