

セキュアエンドポイント：Microsoft攻撃の表面縮小によりコネクタのアップデートがブロックされる

内容

[はじめに](#)

[問題](#)

[回避策](#)

はじめに

このドキュメントでは、Microsoft Intuneによって管理されているシステムで、コピーまたは偽装されたシステムツール機能を使用したMicrosoft Intune攻撃サーフェス削減ブロックによって引き起こされる問題について説明します。これらの機能が原因で、セキュアエンドポイントの更新が失敗します。

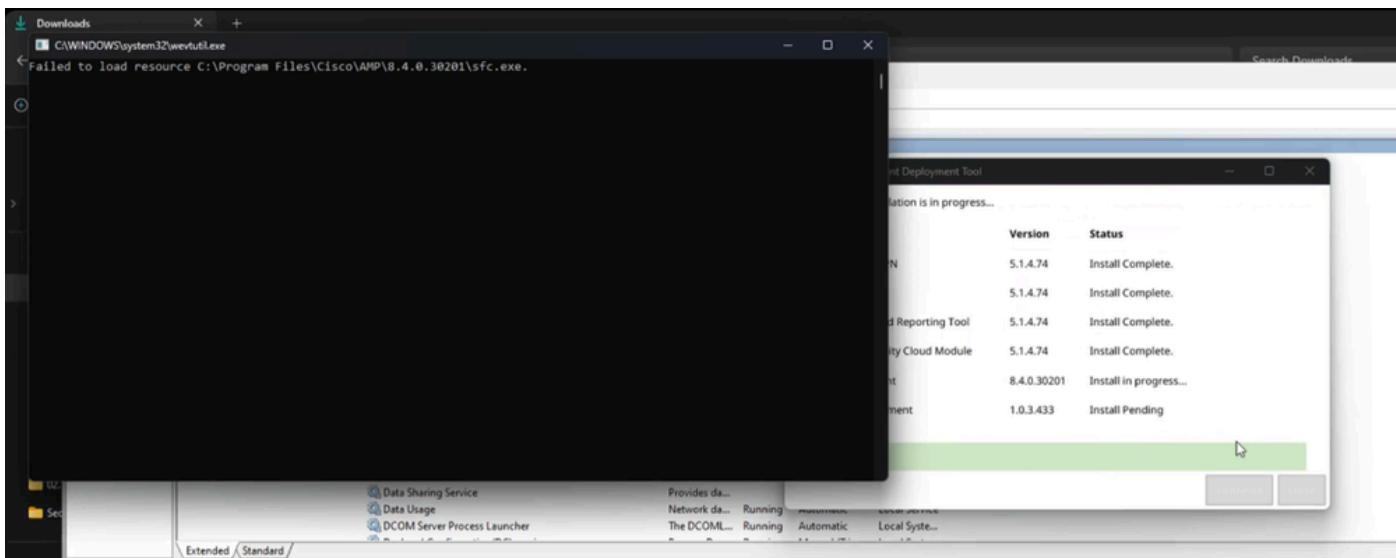
機能のマニュアルを参照してください。 <https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction>

問題

これらのエラーとインジケータに示される、セキュアエンドポイントのアップグレードまたはインストールに関する問題が発生する可能性があります。

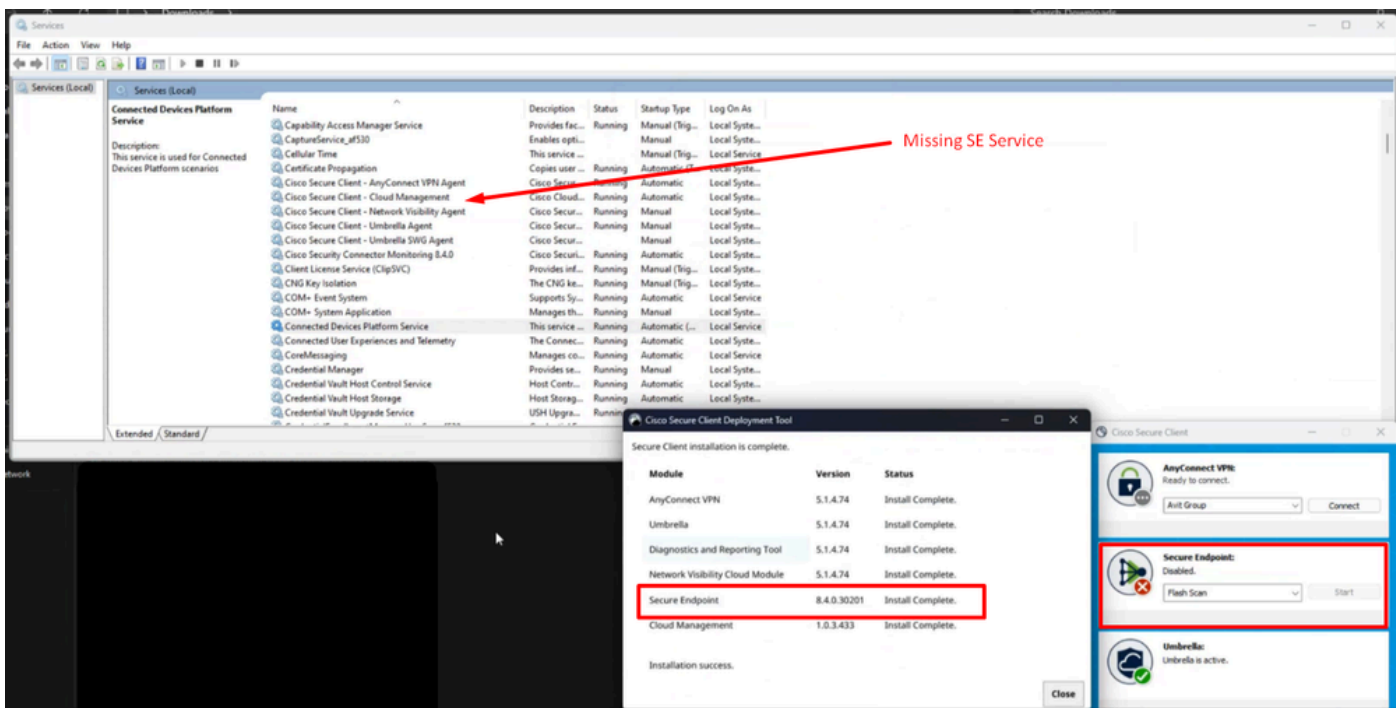
この機能がセキュアエンドポイントのアップデートに干渉していることを特定するために使用できるさまざまなインジケータがあります。

インジケータ#1:導入時に、インストールの最後にこのポップアップウィンドウが表示されます。ポップアップは非常に迅速であり、インストールが完了すると他のエラーの記憶がないことに注意してください。

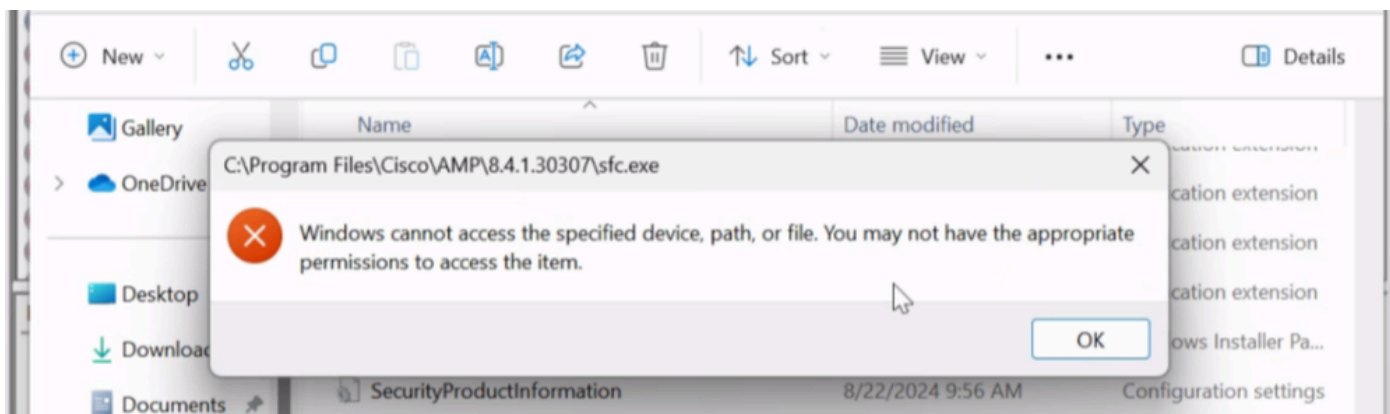


インジケータ#2:インストール後、UIでセキュアエンドポイントが無効状態になっていることに注目してください。

また、タスクマネージャ -> サービスに Secure Endpoint Service(sfc.exe)が完全に見つからない



インジケータ#3: Cisco Secure Endpointの C:\Program Files\Cisco\AMP\バージョンの場所に移動し、サービスを手動で開始しようとする、ローカル管理者アカウントのアクセスが拒否されることがあります



インジケータ#4:診断バンドルの一部であるimpro_install.logを調査すると、次の出力に類似した同様のアクセス拒否が確認できます。

Example #1:

```
(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: Util::GetFileSHA256: unable to generate file fp: C:\Pr  
(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: VerifyFile: Failed to grab hash of C:\Program Files\Ci  
(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: VerifyAllInstalledFiles: Failed to verify $AMP_INSTALL
```

Example #2:


```
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: imn_error: fp_gen_internal: failed to open file C:\Pr  
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: Util::GetFileSHA256: unable to generate file fp: C:\P  
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: VerifyFile: Failed to grab hash of C:\Program Files\C  
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: VerifyAllInstalledFiles: Failed to verify $AMP_INSTAL
```

インジケータ#5:Windowsセキュリティの下を移動し、保護履歴ログを確認する場合は、次のタイプのログメッセージを探します。

Protection history

View the latest protection actions and recommendations from Windows Security.


All recent items


Filters 



Risky action blocked

12/09/2024 06:25

Low 

 Your administrator has blocked this action.

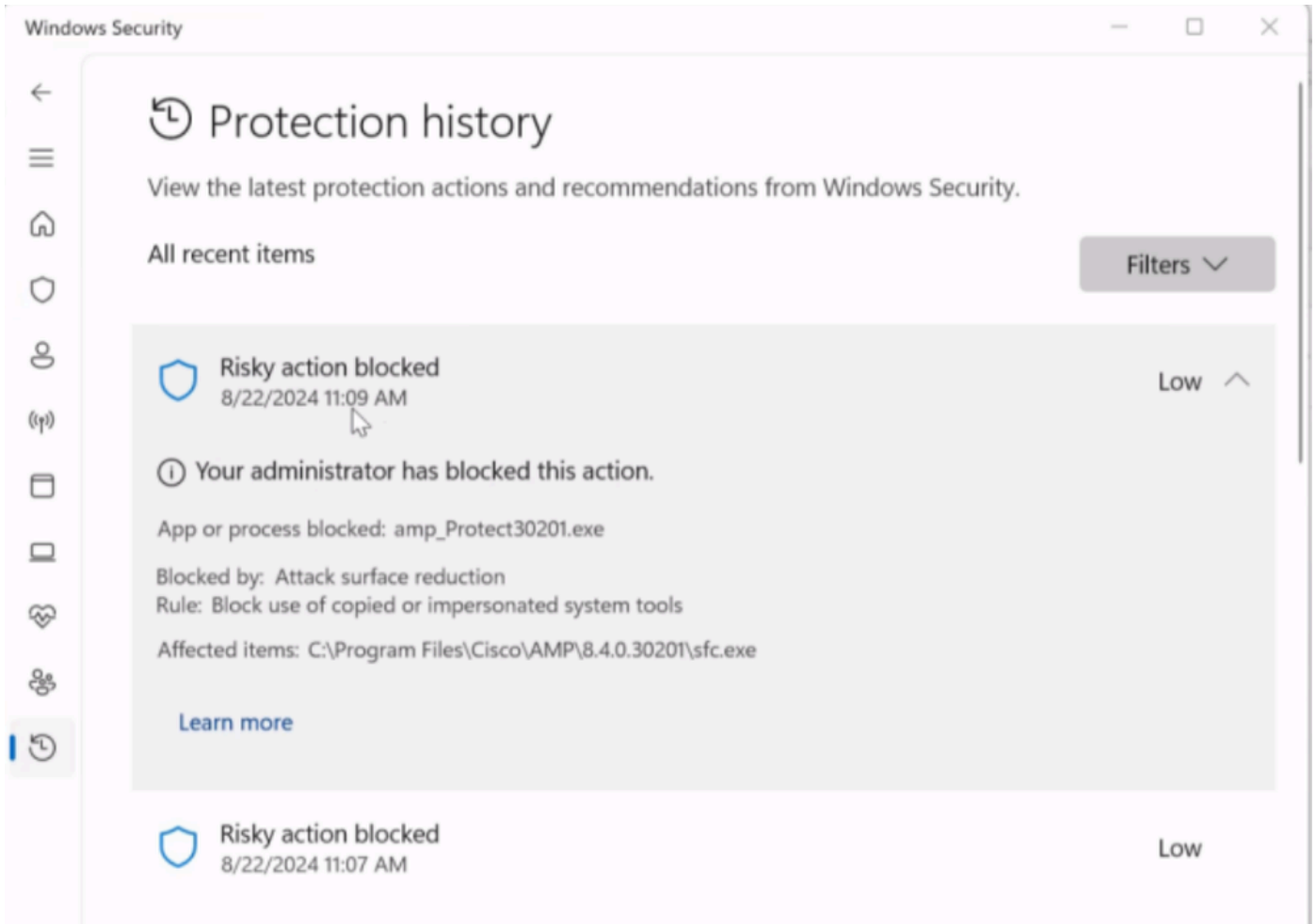
App or process blocked: powershell.exe

Blocked by: Attack surface reduction

Rule: Block use of copied or impersonated system tools

Affected items: C:\Program Files\Cisco\AMP\8.4.2.30317\sfc.exe

[Learn more](#)



これらはすべて、セキュアエンドポイントがサードパーティアプリケーションによってブロックされていることを示しています。このシナリオでは、この問題は、Intune管理対象エンドポイントで誤って構成された、または構成されていない攻撃対象領域の縮小 – コピーまたは偽装されたシステム機能の使用をブロックする機能を使用した場合に発生します。

回避策

この機能の設定については、アプリケーション開発者に相談するか、この[ナレッジベース](#)で詳細を調べることをお勧めします。

すぐに修復するには、Intuneの管理対象エンドポイントを制限の少ないポリシーに移動するか、適切な手順が行われるまで、この機能を一時的に明示的にオフにします。

これは、Intune管理ポータルで、セキュリティで保護されたエンドポイント接続を復元するための一時的な手段として使用された設定です。

Edit profile - WCS - Defender Baseline

Settings catalog

Block Office communication application from creating child processes

Block all Office applications from creating child processes

Block Adobe Reader from creating child processes

Block credential stealing from the Windows local security authority subsystem

Block JavaScript or VBScript from launching downloaded executable content

Block Webshell creation for Servers

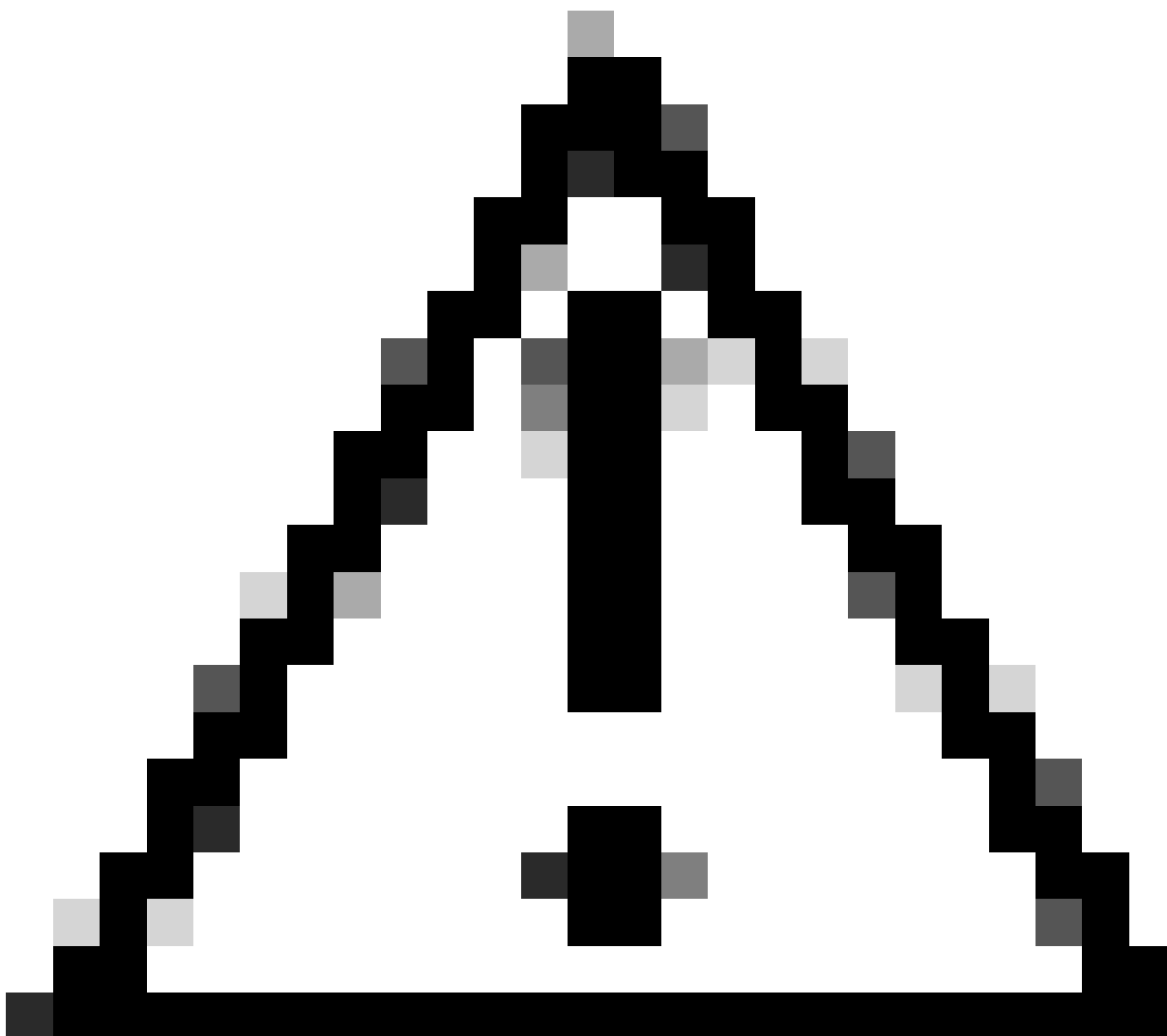
Block trusted and unsigned processes that run from USB

Block persistence through WMI event subscription

[PREVIEW] Block use of copied or impersonated system tools

Block abuse of exploited vulnerable signed drivers (Device)

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support



注意：この問題が発生する場合は、sfc.exeが見つからないため、フルインストールを開始する必要があります

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。