Dépannage de la compatibilité des terminaux sécurisés avec KuTools pour Excel

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Problème

- Dépannage
- Injecter la stratégie modifiée et vérifier
- Appliquer les modifications à l'échelle de l'entreprise

Informations connexes

Introduction

Ce document décrit comment dépanner la compatibilité du module complémentaire tiers appelé KuTools pour Excel avec Secure Endpoint.

Conditions préalables

Exigences

- Accès au portail d'assistance Secure Endpoint
- Connaissances de base de l'administration de Windows (démarrage et arrêt des services)

Il est nécessaire de tester et d'enregistrer ces étapes dans WebEx pour vérifier le fonctionnement avant d'appliquer les modifications à l'échelle de l'entreprise. Il s'agit d'une preuve que vous devez fournir aux escalades.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Portail de support des terminaux sécurisés Cisco v5.4.2022031616
- Cisco Secure Endpoint v7.4.5 et versions ultérieures
- Prévention des exploits, toutes versions
- Windows®10
- Microsoft® Office 365™ Excel®

- KuTools™ pour Excel v26.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

KuTools pour Excel est un module complémentaire tiers conçu pour simplifier, automatiser et étendre les fonctionnalités de Microsoft Excel. Kutools s'intègre avec Microsoft Office 2007 et les versions plus récentes, ainsi qu'Office 365. Une licence d'utilisation du logiciel est requise ; une période d'essai gratuite de 30 jours est offerte sur leur site Web.

Problème

KuTools interagit avec une DLL spécifique appelée wbemdisp.dll. Cela déclenche un événement de prévention des exploits et entraîne le blocage d'Excel.

Lorsque Excel tombe en panne, les événements tels que ceux-ci sont consignés dans la barre d'état et dans la console, ainsi que dans les journaux des événements Windows, comme le montrent ces images :

Dépannage

Pour les étapes suivantes, nous obtenons la stratégie appropriée auprès du portail de support et l'injectons dans le connecteur Secure Endpoint pour tester que cette solution fonctionne réellement.

1. Accédez au portail de support. N'oubliez pas que chaque région possède son propre portail d'assistance.
2. Recherchez l'organisation appropriée. Accédez à Stratégies.
3. Cliquez sur la stratégie appropriée. Vous accédez alors à Détails de la stratégie.
4. Cliquez sur Edit Policy XML en haut à droite de la page. Vous accédez alors à la page Edit Policy XML où vous modifiez la stratégie avant de la télécharger.

Supprimez wbemdisp.dll d'ExPrev V4, sous Script Control Rule EXCEL.EXE.

```
    <v4>

<include_app_list>MicrosoftEdgeCP.exe|browser_broker.exe|msedge.exe|excel.exe|winword.exe|powerpnt.exe|outlook.exe|iexplore.exe|fir
efox.exe|chrome.exe|teamviewer.exe|vlc.exe|wscript.exe|powershell.exe|acrord32.exe|rundll32.exe|taskeng.exe|regsvr32.exe|mshta.exe|c
script.exe|regasm.exe|zoom.exe|skype.exe|slack.exe|CiscoCollabHost.exe|CiscoWebexStart.exe|Teams.exe|C:\Users\*\AppData\Local\Te
mp\*|C:\Users\*\AppData\Roaming\*|eqnedt32.exe</include_app_list>
      <dll_block_list>Windows.Media.Protection.PlayReady.dll|activation2-vc100-mt-s-x86.dll|activation2-vc120-mt-s-
x86.dll|mono.dll|wwlib.dll|chrome_child.dll|oranls11.dll|ChakraCore.dll|NewlyAdded.dll|AnotherNewlyAdded.dll</dll_block_list>
      <exclude_app_list>fcags.exe|mfeepmpk_utility.exe|WebexMTA.exe|atmgr.exe</exclude_app_list>
      <script_control>
        <exclude>test1234.exe</exclude>
        <rule>WINWORD.EXE|wbemdisp.dll|System.Management.Automation.dll|System.Management.Automation.ni.dll</rule>
        <rule>EXCEL.EXE|wbemdisp.dll|System.Management.Automation.dll|System.Management.Automation.ni.dll</rule>
        <rule>POWERPNT.EXE|wbemdisp.dll|System.Management.Automation.dll|System.Management.Automation.ni.dll</rule>
        <rule>OUTLOOK.EXE|wbemdisp.dll|scrobj.dll|System.Management.Automation.dll|System.Management.Automation.ni.dll</rule>
        <rule>REGSVR32.exe|scrobj.dll</rule>
        <audit>0</audit>
      </script_control>
      <folder_white_list/>
      <options>0x0000012B</options>
    </v4>
```

Répétez les mêmes étapes pour ExPrev V5.

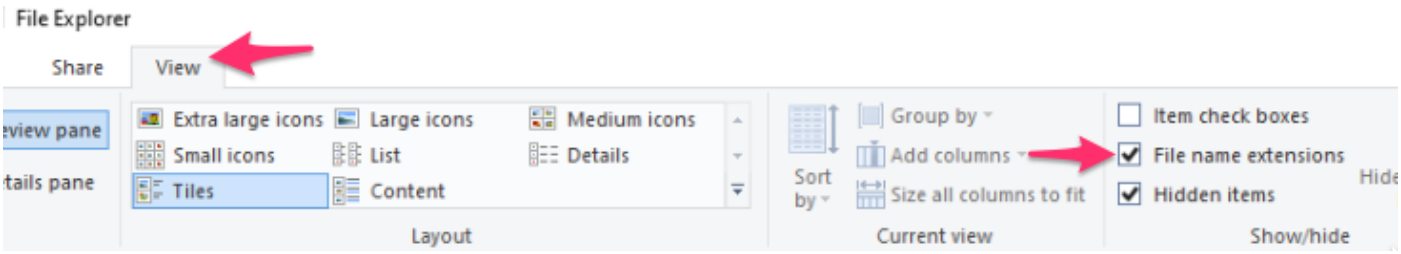
```
    <v5>

<include_app_list>MicrosoftEdgeCP.exe|browser_broker.exe|msedge.exe|excel.exe|winword.exe|powerpnt.exe|outlook.exe|iexplore.exe|fir
efox.exe|chrome.exe|teamviewer.exe|vlc.exe|wscript.exe|powershell.exe|acrord32.exe|rundll32.exe|taskeng.exe|regsvr32.exe|mshta.exe|c
script.exe|regasm.exe|zoom.exe|skype.exe|slack.exe|CiscoCollabHost.exe|CiscoWebexStart.exe|Teams.exe|C:\Users\*\AppData\Local\Te
mp\*|C:\Users\*\AppData\Roaming\*|eqnedt32.exe</include_app_list>
      <dll_block_list>Windows.Media.Protection.PlayReady.dll|activation2-vc100-mt-s-x86.dll|activation2-vc120-mt-s-
x86.dll|mono.dll|wwlib.dll|chrome_child.dll|oranls11.dll|ChakraCore.dll|NewlyAdded.dll|AnotherNewlyAdded.dll</dll_block_list>
      <exclude_app_list>fcags.exe|mfeepmpk_utility.exe|WebexMTA.exe|atmgr.exe</exclude_app_list>
      <script_control>
        <exclude>test1234.exe</exclude>
        <rule>WINWORD.EXE|wbemdisp.dll|System.Management.Automation.dll|System.Management.Automation.ni.dll</rule>
        <rule>EXCEL.EXE|wbemdisp.dll|System.Management.Automation.dll|System.Management.Automation.ni.dll</rule>
        <rule>POWERPNT.EXE|wbemdisp.dll|System.Management.Automation.dll|System.Management.Automation.ni.dll</rule>
        <rule>OUTLOOK.EXE|wbemdisp.dll|scrobj.dll|System.Management.Automation.dll|System.Management.Automation.ni.dll</rule>
        <rule>REGSVR32.exe|scrobj.dll</rule>
        <audit>0</audit>
      </script_control>
      <folder_white_list/>
      <options>0x002EBD2B</options>
    </v5>
  </exprev>
```

Une fois que vous avez fait cela, cliquez sur Download et téléchargez le XML modifié sur votre Cisco Box et créez un lien de partage afin que vous puissiez le télécharger sur le périphérique affecté. Vous pouvez également envoyer le code XML modifié à la personne qui contrôle le périphérique distant par e-mail pendant l'utilisation de WebEx.

Injecter la stratégie modifiée et vérifier

1. Ouvrez services.msc sur la machine concernée.
2. Arrêtez le service Cisco Secure Endpoint <version>.
3. Accédez au chemin d'installation de Secure Endpoint, généralement disponible à l'adresse C:\Program Files\Cisco\AMP\.
4. Recherchez le fichier nommé policy.xml et renommez-le en policy.xml.old. Assurez-vous que les extensions de fichiers sont visibles dans la fenêtre de l'Explorateur. Pour ce faire, cochez la case sous l'onglet Affichage :



1. Collez le fichier XML modifié dans ce dossier.
2. Démarrez le service Cisco Secure Endpoint <version>.

Conseil : si vous tentez de modifier le fichier policy.xml directement à partir du dossier d'installation, le service Cisco Secure Endpoint ne peut pas démarrer.

Vous pouvez maintenant reproduire les étapes qui ont initialement entraîné le test du comportement s'il persiste. Idéalement, KuTools peut prendre un moment, mais fonctionne sans un crash Excel.

Appliquer les modifications à l'échelle de l'entreprise

Une fois que vous avez vérifié que cette solution fonctionne, demandez à vos chefs d'équipe de vous autoriser à la remonter. Assurez-vous que votre demande de service est bien documentée et fournissez toutes les preuves que vous avez recueillies jusqu'à présent pour prouver que la modification d'exclusion résout le comportement. Vous pouvez en savoir plus sur .

Informations connexes

- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.