Risoluzione dei problemi relativi alla compatibilità degli endpoint sicuri con KuTools per Excel

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi di compatibilità del componente aggiuntivo di terze parti noto come KuTools per Excel con Secure Endpoint.

Prerequisiti

Requisiti

- Accesso al portale di supporto Secure Endpoint
- Conoscenze base di Amministrazione di Windows (come avviare e arrestare i servizi)

È necessario eseguire il test e registrare questi passaggi su un WebEx per verificare la funzionalità prima di applicare le modifiche a livello di organizzazione. Questa è la prova che è necessario fornire a Escalations.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Endpoint Support Portal v5.4.2022031616
- Cisco Secure Endpoint v7.4.5 e versioni successive
- Prevenzione degli attacchi, tutte le versioni
- Windows®10
- Microsoft® Office 365™ Excel®

- KuTools™ per Excel v26.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

KuTools per Excel è un componente aggiuntivo di terze parti progettato per semplificare, automatizzare ed espandere le funzionalità di Microsoft Excel. Kutools si integra con Microsoft Office 2007 e versioni più recenti, nonché con Office 365. È necessaria una licenza d'uso del software; sul sito Web è disponibile una versione di prova gratuita di 30 giorni.

Problema

KuTools interagisce con una DLL specifica denominata wbemdisp.dll. In questo modo viene attivato un evento di prevenzione degli attacchi e si verifica il blocco di Excel.

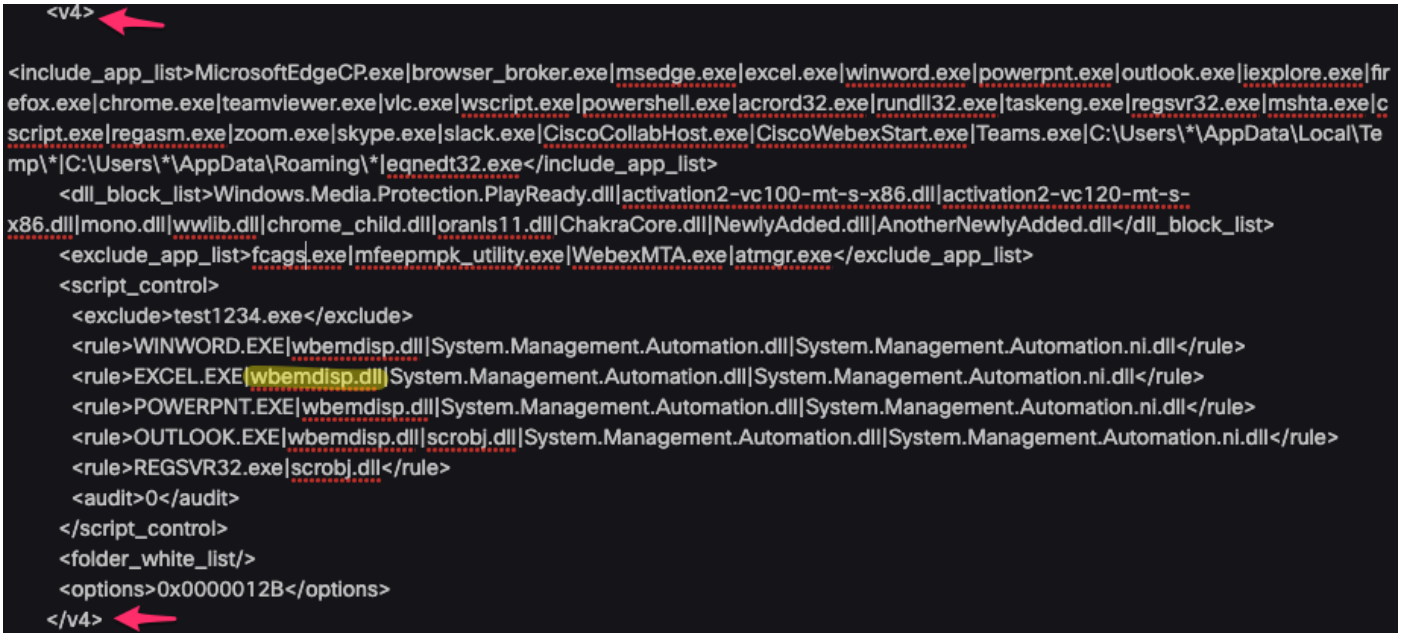
In caso di arresto anomalo di Excel, eventi di questo tipo vengono registrati sia nella barra delle applicazioni che nella console, nonché nei registri eventi di Windows, come illustrato nelle immagini seguenti:

Risoluzione dei problemi

Per le fasi successive, la policy appropriata viene ottenuta dal portale di supporto e immessa nel connettore Secure Endpoint per verificare che questa soluzione funzioni realmente.

1. Accedere al portale di supporto. Tenere presente che ogni area dispone di un proprio portale di supporto.
2. Individuare l'organizzazione rilevante. Vai a Criteri.
3. Fare clic sul criterio pertinente. In questo modo è possibile visualizzare i dettagli della politica.
4. Fare clic su Modifica XML criteri nella parte superiore destra della pagina. Verrà visualizzata la pagina Modifica criterio XML in cui è possibile modificare il criterio prima del download.

Rimuovere wbemdisp.dll da ExPrev V4, in Excel.EXE della regola di controllo dello script.



Ripetere la stessa procedura per ExPrev V5.

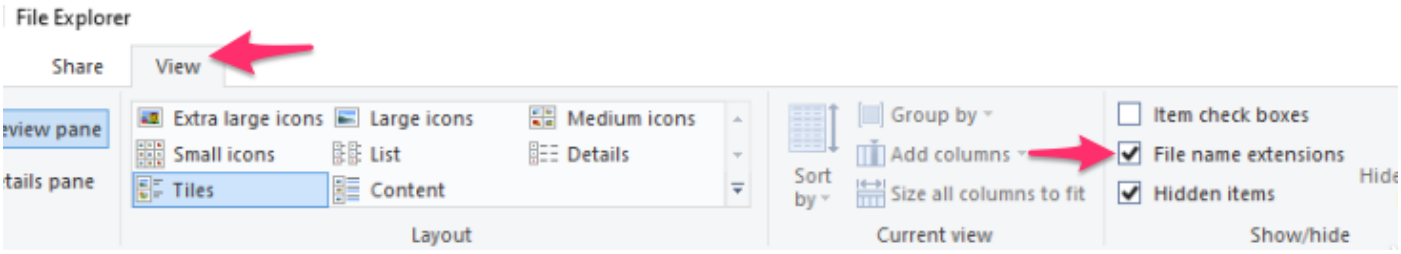
```
    <v5>

<include_app_list>MicrosoftEdgeCP.exe|browser_broker.exe|msedge.exe|excel.exe|winword.exe|powerpnt.exe|outlook.exe|iexplore.exe|firefox.exe|chrome.exe|teamviewer.exe|vlc.exe|wscript.exe|powershell.exe|acrord32.exe|rundll32.exe|taskeng.exe|regsvr32.exe|mshta.exe|cscript.exe|regasm.exe|zoom.exe|skype.exe|slack.exe|CiscoCollabHost.exe|CiscoWebexStart.exe|Teams.exe|C:\Users\*\AppData\Local\Temp\*|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>
```

Al termine, fare clic su Download e caricare il file XML modificato nella Cisco Box per creare un collegamento di condivisione che consenta di scaricarlo sul dispositivo interessato. È inoltre possibile inviare il codice XML modificato alla persona che controlla il dispositivo remoto tramite posta elettronica durante il WebEx.

Inserisci criterio modificato e verifica

1. Aprire services.msc nel computer interessato.
2. Arrestare il servizio Cisco Secure Endpoint <version>.
3. Passare al percorso di installazione di Secure Endpoint, in genere disponibile in C:\Program Files\Cisco\AMP\.
4. Individuare il file policy.xml e rinominarlo in policy.xml.old. Verificare che le estensioni dei file siano visibili nella finestra Esplora risorse. A tale scopo, selezionare la casella di controllo nella scheda Visualizza:



1. Incollare il file XML modificato in questa cartella.
2. Avviare il servizio Cisco Secure Endpoint <version>.

Suggerimento: se si tenta di modificare il file policy.xml direttamente dalla cartella di installazione, non è possibile avviare il servizio Cisco Secure Endpoint.

È ora possibile riprodurre i passaggi che hanno inizialmente determinato il test del comportamento se persiste. In teoria, KuTools potrebbe impiegare un po' di tempo, ma funziona senza un arresto anomalo di Excel.

Applica modifiche a livello di organizzazione

Dopo aver verificato il corretto funzionamento di questa soluzione, richiedere l'autorizzazione ai responsabili del team per l'escalation. Assicurarsi che la SR sia ben documentata e fornire tutte le prove raccolte fino ad ora per dimostrare che la modifica dell'esclusione risolve il comportamento. Ulteriori informazioni su .

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).