排除安全終端與Excel庫工具相容的故障

目錄

簡介

本文檔介紹如何對第三方載入項（稱為KuTools for Excel with Secure Endpoint）的相容性進行故障排除。

必要條件

需求

- 訪問安全終端支援門戶
- Windows管理的基本知識（如何啟動和停止服務）

在WebEx上測試並記錄這些步驟後，必須在全組織範圍內應用更改之前驗證功能。 這是您需要向Escalation提供的證據。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全終端支援門戶v5.4.2022031616
- Cisco Secure Endpoint v7.4.5及更高版本
- 防漏洞攻擊，所有版本
- Windows®10
- Microsoft® Office 365™ Excel®
- 適用於Excel v26.0的KuTools™

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

KuTools for Excel是第三方外掛，旨在簡化、自動化和擴展Microsoft Excel的特性和功能。 Kutools可與Microsoft Office 2007和更新版本以及Office 365整合。 使用該軟體需要許可證；其網站提供為期30天的免費試用版。

問題

KuTools與名為wbemdisp.dll的特定DLL互動。這將觸發漏洞防護事件，並導致Excel崩潰。

當Excel崩潰時，系統會在系統匣和主控台中記錄類似的事件，以及Windows事件記錄檔，如以下影像所示：

疑難排解

對於後續步驟，我們從支援門戶獲取相關策略，並將其注入安全終端聯結器以測試此解決方案是否真正有效。

1. 轉到支援門戶。請記住，每個區域都有自己的支援門戶。
2. 查詢相關組織。轉到Policies。
3. 點選相關策略。這會顯示策略詳細資訊。
4. 按一下頁面右上方的Edit Policy XML。這會顯示Edit Policy XML頁面，您可以在此頁面修改策略後再下載。

在指令碼控制規則EXCEL.EXE下，從ExPrev V4刪除wbemdisp.dll。

```
<v4>
<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>0x0000012B</options>
</v4>
```

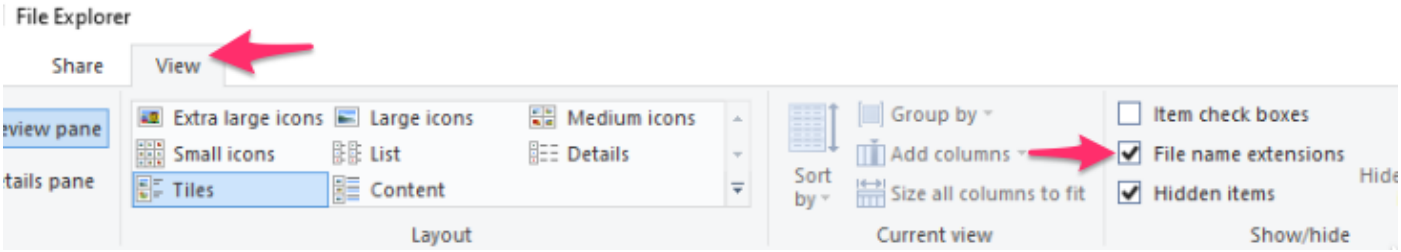
對ExPrev V5重複相同的步驟。

```
<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>
```

完成後，點選下載，然後將修改的XML上傳到Cisco Box並建立共用連結，以便您能夠將其下載到受影響的裝置上。您也可以在WebEx期間透過電子郵件將修改後的XML傳送給遠端裝置控制人員。

插入修改後的策略並進行驗證

1. 在受影響的電腦上打開services.msc。
2. 停止Cisco Secure Endpoint <version>服務。
3. 轉到安全終端的安裝路徑，通常位於C:\Program Files\Cisco\AMP\。
4. 查詢名為policy.xml的檔案，並將其重新命名為policy.xml.old。確保在Explorer窗口中顯示副檔名。可以透過選中View頁籤下的框來執行此操作：



1. 將修改的XML貼到此資料夾中。
2. 啟動Cisco Secure Endpoint <version>服務。

提示：如果嘗試直接從安裝資料夾修改policy.xml，思科安全終端服務將無法啟動。

現在，您可以重現最初導致行為測試持續性的步驟。理想情況下，KuTools可以花一點時間，但運行時不發生Excel崩潰。

在全組織範圍內套用變更

驗證此解決方法有效後，請獲得團隊領導授權，以便上報。確保您的SR有詳細的文檔記錄，並提供您到目前為止收集的所有證據，以證明排除修改解決了此行為。您可以閱讀更多關於。

相關資訊

- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。