对安全终端与KuTools for Excel的兼容性进行故障排除

目录

简介

本文档介绍如何对名为KuTools for Excel的第三方加载项与安全终结点的兼容性进行故障排除。

先决条件

要求

- 访问安全终端支持门户
- Windows管理基础知识（如何启动和停止服务）

在全组织范围应用更改之前，需要在WebEx上测试和记录这些步骤，以验证功能。 这是您需要为升级提供的证据。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全终端支持门户v5.4.2022031616
- 思科安全终端v7.4.5及更高版本
- 漏洞防御，所有版本
- Windows®10
- Microsoft® Office 365™ Excel®
- 用于Excel v26.0的KuTools™

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

KuTools for Excel是第三方插件，旨在简化、自动化和扩展Microsoft Excel的特性和功能。 Kutools可与Microsoft Office 2007和更新版本以及Office 365集成。 使用该软件需要许可证；他们的网站上提供了免费的30天试用版。

问题

KuTools与名为wbemdisp.dll的特定DLL交互。这会触发漏洞防御事件并导致Excel崩溃。

当Excel崩溃时，这些事件（例如这些事件）会记录在任务栏和控制台，以及Windows事件日志中，如以下图像所示：

故障排除

对于后续步骤，我们从支持门户获取相关策略，并将其注入安全终端连接器，以测试此解决方案是否真正有效。

1. 转到支持门户。请记住，每个地区都有自己的支持门户。
2. 查找相关组织。转到Policies。
3. 点击相关策略。这会显示Policy Details。
4. 单击页面右上方的Edit Policy XML。这会显示Edit Policy XML页，您可以在该页中修改策略后再下载。

在脚本控制规则EXCEL.EXE下，从ExPrev V4删除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>
```

对ExPrev V5重复相同的步骤。

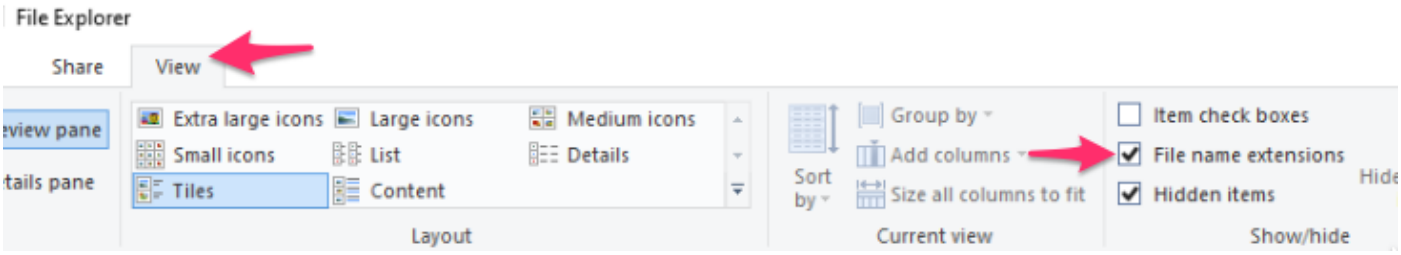
```
<v5>
<include_app_list>MicrosoftEdgeCP.exe|browser_broker.exe|msedge.exe|excel.exe|winword.exe|powerpnt.exe|outlook.exe|iexplore.exe|firefox.exe|chrome.exe|teamviewer.exe|vlc.exe|wscript.exe|powershell.exe|acrord32.exe|rundll32.exe|taskeng.exe|regsvr32.exe|mshta.exe|cscript.exe|regasm.exe|zoom.exe|skype.exe|slack.exe|CiscoCollabHost.exe|CiscoWebexStart.exe|Teams.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>
```

完成后，单击Download并将修改的XML上载到Cisco Box并创建一个共享链接，以便您可以将它下载到受影响的设备上。在WebEx会议期间，您还可以通过电子邮件将修改后的XML发送给控制远程设备的人员。

插入修改后的策略并进行验证

1. 在受影响的计算机上打开services.msc。
2. 停止Cisco Secure Endpoint <version>服务。
3. 转到安全终端的安装路径，通常位于C:\Program Files\Cisco\AMP\。
4. 查找名为policy.xml的文件，并将其重命名为policy.xml.old。确保在“资源管理器”窗口中可以看

到文件扩展名。要执行此操作，请选中View选项卡下的复选框：



1. 将修改后的XML粘贴到此文件夹中。
2. 启动Cisco Secure Endpoint <version>服务。

提示：如果您尝试直接从安装文件夹修改policy.xml，思科安全终端服务将无法启动。

现在，您可以复制最初导致该行为的步骤，以测试该行为是否仍然存在。理想情况下，KuTools可以花一些时间，但运行时不会出现Excel崩溃。

在整个组织范围应用更改

验证此解决方法有效后，请获得团队主管的授权以升级。确保您的SR记录完备，并提供您到目前为止收集到的所有证据，以证明排除修改解决了此行为。有关详细信息，请参阅。

相关信息

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。