

Troubleshoot Secure Endpoint Compatibility with KuTools for Excel

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Problem](#)

[Troubleshoot](#)

[Inject Modified Policy and Verify](#)

[Apply Changes Organization-Wide](#)

[Related Information](#)

Introduction

This document describes how to troubleshoot compatibility of the third party add-on known as KuTools for Excel with Secure Endpoint.

Prerequisites

Requirements

- Access to Secure Endpoint Support Portal
- Basic knowledge of Windows Administration (how to start and stop services)

It is required to test and record these steps while on a WebEx to verify functionality before you apply the changes Organization-wide. This is evidence you are required to provide to Escalations.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Endpoint Support Portal v5.4.2022031616
- Cisco Secure Endpoint v7.4.5 and greater
- Exploit Prevention, all versions
- Windows®10
- Microsoft® Office 365™ Excel®
- KuTools™ for 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

KuTools for Excel is a third party add-on designed to simplify, automate, and expand the features and functions of Microsoft Excel. Kutools integrates with Microsoft Office 2007 and newer versions, as well as Office 365. A license to use the software is required; a free 30 day trial is offered on their website.

Problem

KuTools interacts with a specific DLL called **wbemdisp.dll**. This triggers an Exploit Prevention event and causes Excel to crash.

When Excel crashes, events such as these are logged in both Tray and Console, as well as Windows Event Logs as seen in these images:



Troubleshoot

For the next steps, we obtain the relevant policy from Support Portal and inject it onto the Secure Endpoint connector to test that this solution actually works.

1. Go to **Support Portal**. Remember that each region has its own support portal.
2. Find the relevant Organization. Go to **Policies**.
3. Click the relevant policy. This takes you to **Policy Details**.
4. Click **Edit Policy XML** at the top right of the page. This takes you to the **Edit Policy XML** page where you modify the Policy prior to download.

Remove **wbemdisp.dll** from **ExPrev V4**, under **Script Control Rule EXCEL.EXE**.

```
<v4>
<include_app_list>MicrosoftEdgeCP.exe|browser_broker.exe|msedge.exe|excel.exe|winword.exe|powerpnt.exe|outlook.exe|explore.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|orans11.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>
```

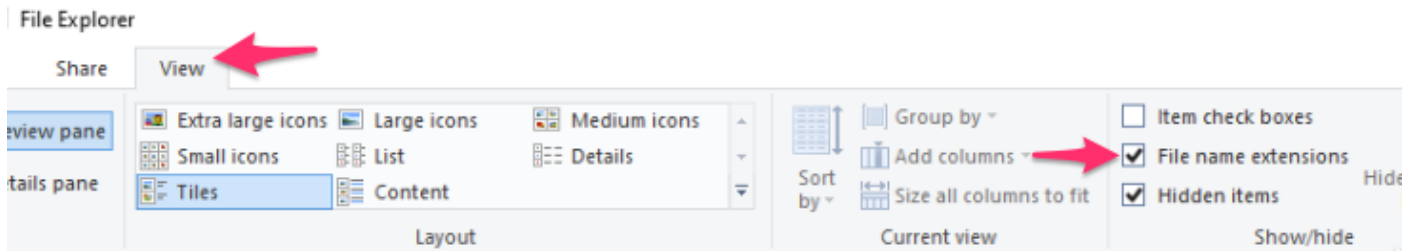
Repeat the same steps for ExPrev V5.

```
<v5>
<include_app_list>MicrosoftEdgeCP.exe|browser_broker.exe|msedge.exe|excel.exe|winword.exe|powerpnt.exe|outlook.exe|explore.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|orans11.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>
```


Once you have done this, click **Download** and upload the modified XML to your [Cisco Box](#) and create a share link so you can download it on the affected device. You can also send the modified XML to the person in control of the remote device via e-mail during the WebEx.

Inject Modified Policy and Verify

1. Open services.msc on the affected machine.
2. Stop the Cisco Secure Endpoint <version> service.
3. Go to the installation path for Secure Endpoint, usually located at C:\Program Files\Cisco\AMP\.
4. Find the file named **policy.xml** and rename it to **policy.xml.old**. Make sure you have file extensions visible on the Explorer window. You can do this by checking the box under **View** tab:



1. Paste the modified XML in this folder.
2. Start the Cisco Secure Endpoint <version> service.

 **Tip:** If you attempt to modify the policy.xml directly from the installation folder, the Cisco Secure Endpoint service cannot start.

Now you can reproduce the steps that initially caused the behavior to test if it persists. Ideally, KuTools can take a moment but runs without an Excel crash.

Apply Changes Organization-Wide

Once you have verified this workaround works, obtain authorization from your Team Leads to escalate. Ensure your SR is well documented and provide all the evidence you have gathered so far to prove that the exclusion modification resolves the behavior. You can read more about .

Related Information

- [Technical Support & Documentation - Cisco Systems](#)