
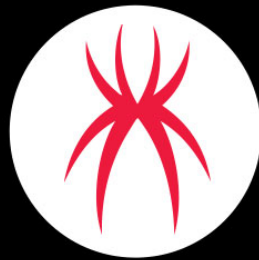


Trustwave's Action Response: Microsoft zero-day CVE-2022-30190 (aka Follina)

 trustwave.com/en-us/resources/blogs/spiderlabs-blog/trustwaves-action-response-microsoft-zero-day-cve-2022-30190-aka-follina



SpiderLabs Blog

Loading...

Blogs & Stories

SpiderLabs Blog

Attracting more than a half-million annual readers, this is the security community's go-to destination for technical breakdowns of the latest threats, critical vulnerability disclosures and cutting-edge research.

*Update June 7 - In the event of a compromise related to the Follina vulnerability, IT teams can potentially identify network connections in the registry associated with the malicious Office document. Additionally, spawned child processes might also be identified in the diagnostic PCW.debugreport.xml file on the host. Please see **Hunting for Indicators of Compromise** below for more details.*

Trustwave SpiderLabs is tracking the critical-rated zero-day vulnerability CVE-2022-30190. Threat actors are reported to be actively exploiting this vulnerability in the wild. Microsoft disclosed and issued guidance for CVE-2022-30190 on May 30.

Trustwave is diligently watching over our clients for exposure and associated attacks and working closely with our clients to ensure that mitigations are in place. Trustwave SpiderLabs is continuing to monitor this developing threat and we will update this blog as necessary.

Over Memorial Day weekend a zero-day vulnerability was discovered being actively exploited in the wild. The initial sample was a malicious Microsoft Word document that triggered arbitrary code execution when opened. Microsoft has issued this vulnerability **CVE-2022-30190**, but it is also known as "**Follina**".

Overview

The vulnerability is an issue with the Microsoft Support Diagnostic Tool (MSDT) in Windows. The initial attack vector used a Word document that used the remote template feature to retrieve an HTML file from a remote webserver. The HTML file invokes "ms-msdt" MSProtocol URI scheme to load some code and execute some PowerShell.

This vulnerability potentially affects any Office document that has access to MSDT. For instance, if the document is a .RTF file, it becomes a zero-click exploit if Preview in Explorer is enabled. Outlook also supports MS Protocol URI schemes, e.g. "ms-msdt:some_uri/resource" which would trigger exploitation if clicked.

The full attack surface and all exploitation methods have not yet been completely explored. While the original exploit only seemed to affect MS Word, additional research resulted in attack vectors expanding to include the RTF and potential Outlook vectors.

As of June 2, an additional attack vector was discovered that invokes a "search-ms" URI instead of "ms-msdt" to achieve the same effect of arbitrary code. With the "search-ms" variant, the attacker invokes the Windows Search functionality to launch a malicious Word document.

Remediation for MSDT exploitation

The vulnerability affects Office 2013, 2016, 2019, 2021, Office ProPlus and Office 365. As of this writing, there is no patch available, but we anticipate Microsoft will release one in short order. In the meantime, Microsoft provides the following workarounds:

Disable the MSDT URL Protocol

- Run Command Prompt as Administrator.
- To back up the registry key, execute the command "reg export HKEY_CLASSES_ROOT\ms-msdt filename"
- Execute the command "reg delete HKEY_CLASSES_ROOT\ms-msdt /f".

How to Undo the Workaround

- Run Command Prompt as Administrator.
- To restore the registry key, execute the command "reg import filename" pointing to the backup file you created before disabling MSDT

Remediation for "search-ms" exploitation

Like the remediation for "ms-msdt", this remediation disables search-ms via the registry. Microsoft provide the following workarounds:

Disable the "ms-search" URL Protocol

- Run Command Prompt as Administrator.
- To back up the registry key, execute the command "reg export HKEY_CLASSES_ROOT\search-ms filename"
- Execute the command "reg delete HKEY_CLASSES_ROOT\search-ms /f".

How to Undo the Workaround

- Run Command Prompt as Administrator.
- To restore the registry key, execute the command “reg import filename” pointing to the backup file you created in the previous section.

However, these workarounds may cause issues depending on the environment and local usage of MSDT and “search-ms.” It also does not mitigate some attack vectors like automatic preview in Explorer of malicious RTF documents. In cases where this mitigation step is not implementable, utilizing existing endpoint protection solutions for blocking and or detection is the best course of action. Multiple vendors have already released guidance for their solutions to defend or detect this exploitation.

Hunting for Indicators of Compromise

In the event of a compromise related to the Follina vulnerability, IT teams can potentially identify network connections in the registry associated with the malicious Office document. Additionally, spawned child processes might also be identified in the diagnostic PCW.debugreport.xml file on the host.

In some instances, a registry value will be created if an Office document attempting to utilize the Follina vulnerability, makes an Internet connection. Though this could identify a C2 server, not every instance of a malicious Office document executing on a machine will result in a network connection as this can be dependent upon the payload. There could also be a large number of entries, as the registry keys are historical and not removed after the machine reboots. This will require further investigation into the domains observed in the registry to determine if they are associated with malicious behaviors.

HKEY_USERS\%USER_SID%\SOFTWARE\Microsoft\Office\%OFFICE_VERSION\Common\Internet\Server Cache\

HKCU\Software\Microsoft\Office\%OFFICE_VERSION\Common\Internet\Server Cache\Count\

During an investigation or post compromise DFIR engagement, the registry can be checked via EDR technologies that allow for registry queries or can be checked by remotely connecting to the machine and running the PowerShell commands below:

```
Get-ChildItem -Path 'HKCU:\SOFTWARE\Microsoft\Office\16.0\Common\Internet\Server Cache\'
```

```
Get-ChildItem
```

```
'Registry::HKEY_USERS\%USER_SID%\SOFTWARE\Microsoft\Office\%OFFICE_VERSION\Common\Internet\Server Cache\'
```

Another file to check that can identify the potential child / spawned processes is the PCW.debugreport.xml file located here.

```
C:\Users[USERNAME]\AppData\Local\Diagnostics\[randomnumber]\[randomnumber].  
[xxx]\PCW.debugreport.xml
```

Within the XML file, the value '<Data id="Parameter" name="TargetPath">[string]\' can contain the path of the executed process or executable.

References

MSRC blog post: <https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/>

Original analysis: <https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerability-1a47fce5629e>

Non-malicious Word doc PoC for testing: <https://app.box.com/s/9oz1r90tzs7bstl0xy3zzfc8m92cqhc>

Attack variant using “search-ms”: <https://borncity.com/win/2022/06/02/searchnightmare-windows-10-search-ms-uri-handler-0-day-exploit-mit-office-2019/>

Office network connections in the registry:

<https://twitter.com/SecurityAura/status/1531337827019014144>

PCW.debugreport.xml

https://twitter.com/NOP_0x90v1/status/1532983486591774721

<https://twitter.com/wdormann/status/1532080950708170752>

Yara Rule - <https://docs.velociraptor.app/exchange/artifacts/pages/msdtfollina/>

Trustwave

The Trustwave SpiderLabs IDS team released five IDS signatures as an out of band release to cover known attack vectors. The Trustwave Global Threat Operations team has also deployed detection rules in the Trustwave Fusion platform. Other Trustwave SpiderLabs teams are still investigating additional protections and detections we can implement.

We will update this blog post as appropriate.