

Forum:[Hack Forums](#)

Thread: [CVE-2022-30190 \[MSDT\] aka Follina Vulnerability - Windows Protection Script](#)

Trillium - June 12, 2022, 6:27 pm

Greetings Guys,

Since the disclosure of CVE-2022-30190 [MSDT] aka Follina Exploit occurred I want to provide you a Windows Protection Script which will protect you against the CVE-2022-30190 [MSDT] aka Follina Exploit!

The Scripts are in 2 Parts.

1. CVE-2022-30190 Windows Protection Script - Backup and Delete

Code @Echo off

:start

echo CVE-2022-30190 [MSDT] aka Follina Vulnerability - Windows Protection Script

echo The Protection Script will create a Registry Backup of the MSDT URL Protocol Registry Entry and then it will delete the MSDT URL Protocol Registry Entry.

echo The Protection Script need to be run as Administrator!

echo You can stop the Protection Script by pressing the keys CTRL-C

echo Enter the Filename for the Registry Backup File.

echo Example: Backup.reg

echo The Registry Backup File will be saved in the same folder location where the Protection Script is located.

set /p backupfilename=Please enter the Registry Backup Filename:

if "%backupfilename%"==" " goto :start

reg export HKEY_CLASSES_ROOT\ms-msdt "%backupfilename%" || goto error

echo The Registry Backup File got successfully saved!

echo Registry Backup File Location:

set CurrentPath=%cd%

set FullFilePath=%CurrentPath%\%backupfilename%

echo %FullFilePath%

:start2

echo The MSDT URL Protocol Registry Entry get now delete!

:choice

set /P c=Are you sure you want to continue[Y/N]?

if /I "%c%" EQU "Y" goto :delete

if /I "%c%" EQU "N" goto :close

goto :choice

:delete

reg delete HKEY_CLASSES_ROOT\ms-msdt /f || goto error2

echo The MSDT URL Protocol Registry Entry got successfully delete!

echo The Protection Script get now closed!

pause

exit

:close

echo The Protection Script get now closed!

```
pause
exit
:error
echo Error
goto start
:error2
echo Error
goto start2
```

Please create on your Desktop a new Text Document File and copy and paste this code into the Text Document File and rename and save it to "Backup and Delete Script.bat".

If you execute this file then a Backup File of the MSDT URL Protocol Registry Entry will get created and the MSDT URL Protocol Registry Entry will get delete.

The CVE-2022-30190 Windows Protection Script - Backup and Delete need to be run as Administrator!

2. MSDT URL Protocol Registry Entry - Restore Script

```
Code @Echo off
:start
echo MSDT URL Protocol Registry Entry - Restore Script
echo The MSDT URL Protocol Registry Entry - Restore Script need to be run as Administrator!
echo You can stop the MSDT URL Protocol Script by pressing the keys CTRL-C
set /p backupfilepath=Please enter the MSDT URL Protocol Registry Backup File Path:
if "%backupfilepath%"==" " goto :start
reg import "%backupfilepath%" || goto :error
echo The MSDT URL Protocol Registry Entry got successfully restored!
echo The MSDT URL Protocol Restore Script get now closed!
pause
exit
:error
echo Error
echo The MSDT URL Protocol Registry Entry - Restore Script get now closed!
pause
exit
```

Please create on your Desktop a new Text Document File and copy and paste this code into the Text Document File and rename and save it to "Restore Script.bat".

If you execute this file then you can select the MSDT URL Protocol Registry Entry Backup File and the MSDT URL Protocol Registry Entry will get restored.

The MSDT URL Protocol Registry Entry - Restore Script need to be run as Administrator!

<https://beebom.com/how-fix-microsoft-follina-msdt-windows-zero-day-vulnerability/>

If someone have any questions or if someone need any help then feel free to contact me anytime!?

Bastille - June 13, 2022, 5:24 am

Thanks for the script buddy ?

Thanks for being active in the White Hat forum as well

Trillium - June 13, 2022, 7:13 am

(Jun 13, 2022 05:24 AM)Yseurk Wrote: [CITE](#) Thanks for the script buddy ?

Thanks for being active in the White Hat forum as well

Greetings Yseurk, no problem its a pleasure for me to help and thank you so much for your positive reply I very appreciate it! If interest should be exists I can also provide a small Executable Program with a GUI which will do the things like the CVE-2022-30190 aka Follina Windows Protection Script + a option to check if the CVE-2022-30190 aka Follina Vulnerability is available on the specific Test-System (Check if MSDT URL Protocol Registry Entry is existing).?