



CYBANETIX SECURITY UPDATE

PRINTNIGHTMARE CVE-2021-1675/

I'm sure you've seen the headlines at the moment about the latest Microsoft security vulnerability, named "Print-Nightmare".

Thus far Microsoft have failed to address the issue with two out of sequence patch releases. Here at Cybanetix, we have dissected the vulnerability and can share with you our findings, along with ways to mitigate, detect and secure your networks. This article designed to be factual and to provide some perimeter information around the print nightmare problem.

Firstly, the vulnerability appears to only be exploitable by a domain user, so this does provide a little bit of protection – but not enough. User credentials can be phished, and even if you use Multi-Factor Authentication it will not provide protection because the exploit is accessed via Samba/CIFS.

MICROSOFT PATCH NUMBER 1

The way the exploit works is by "tricking" the print service to update and then load a user-supplied potentially malicious DLL. So long as the DLL is accessible from the Print Service then the Print Service will load it.

As part of updating print device drivers, three files are provided: A Data File, a Config File and a Driver Path.

As part of the normal operation of performing printer driver updates, the Print service would copy any of these files from the user-supplied UNC path into:

```
C:\Windows\System32\spool\drivers\x64\3\New
```

Following copy these files load the DLL directly into the spoolsv.exe process, which runs with SYSTEM privileges. From here, the malicious code can go on to create a domain user with full admin privileges, allowing an attacker to gain full control over the entire Windows domain.

Microsoft initially patched this vulnerability by restricting the location of the Data file and Driver Path so that these could no longer be UNC paths, however, this was not enough protection.

If two separate driver update requests were made, the first one specifying UNC path to a DLL for the “Config” file parameter, the print service would still happily copy the DLL from the UNC path into the local file system, but would then fail.

A second driver update request could then be made specifying the local DLL file that was copied from the previous request.

The outcome of this could potentially be the execution of malicious code making the patch invalid.

MICROSOFT PATCH NUMBER 2

On the 7th July, Microsoft released a new patch which provides the better protection against this vulnerability.

The patch and related information is available at the following URL: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>

However, there are some reports that the patch has failed to provide 100% protection as per this report from Ars Technica – specifically where users have “Point and Print” enabled.

To mitigate against this particular attack the following recommendations should be followed:-

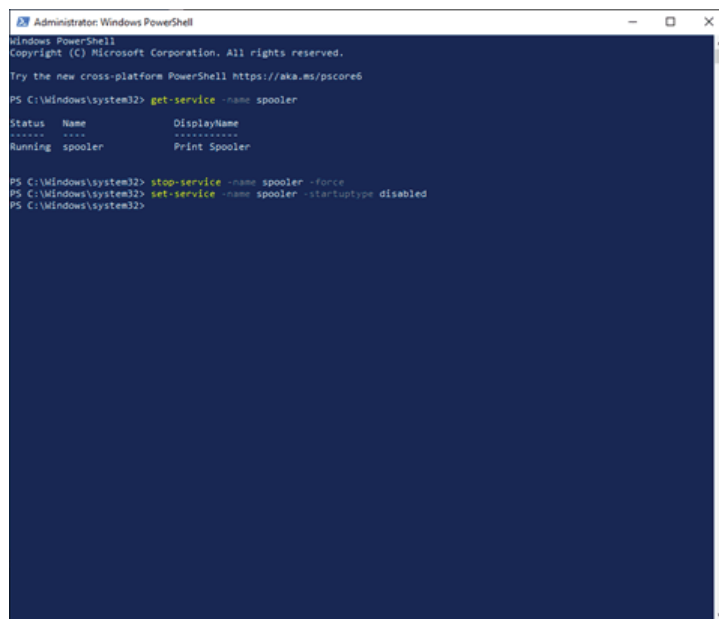
1) Install the patch provided by Microsoft and ensure all other parts of the system are up to date.

2) Delete following registry keys or set their value to 0 (zero)

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
- NT\Printers\NoWarningNoElevationOnInstall
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\UpdatePromptSettings

3) Disable the print spooler service (Run powershell as administrator)

- Check if the spooler is running in powershell `Get-Service -Name Spooler`
- Stop the spooler service `Stop-Service -Name Spooler -Force`
- Disable the spooler service on startup `Set-Service -Name Spooler -StartupType Disabled`



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> get-service -name spooler

Status Name      DisplayName
-----
Running spooler      Print Spooler

PS C:\Windows\system32> stop-service -name spooler -force
PS C:\Windows\system32> set-service -name spooler -startuptype disabled
PS C:\Windows\system32>
```

4) Make it impossible for new drivers to be written into the folder exploited

- mkdir “C:\Windows\System32\spool\drivers\x64\3\New”
- Make the exploit path immutable
- icacls “C:\Windows\System32\spool\drivers\x64\3\New” /deny everyone:(OI)(CI)(DE,DC,WD,AD)

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.1052]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>mkdir C:\Windows\System32\spool\drivers\x64\3\New

C:\WINDOWS\system32>icacls C:\Windows\System32\spool\drivers\x64\3\New /deny everyone:(OI)(CI)(DE,DC,WD,AD)
processed file: C:\Windows\System32\spool\drivers\x64\3\New
Successfully processed 1 files; failed processing 0 files

C:\WINDOWS\system32>
```

Please be aware that the attack surface identified in print nightmare is likely to garner a growing collection of exploits over the coming months and years, as such we recommend that unless absolutely necessary the print spooler service should remain in the disabled state, with the immutable exploit path until the issues surrounding this service have been fully mitigated by Microsoft. If you must use the print spooler then we suggest that you ensure that all the required drivers are already installed on the affected workstations and that the driver path is made immutable with the command provided in recommended action.

FOR CYBANETIX CUSTOMERS

There are several ways in which you can check that you have not already been attacked. The exact way to check will depend on which technology stack you are using, so please read on for more details.

(If you have a SOC service from us, then we are already doing this for you).

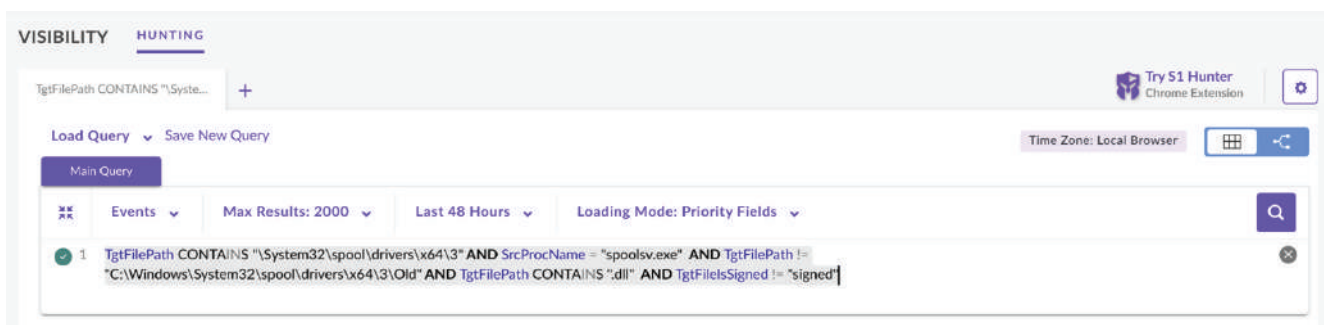
SENTINOLE ONE

For S1 users, you can look for file writes to the “C:\Windows\System32\spool\drivers\x64\3\New” directory with the following Deep Vis query:

```
TgtFilePath CONTAINS "\System32\spool\drivers\x64\3" AND SrcProcName = "spoolsv.exe" AND TgtFilePath != "C:\Windows\System32\spool\drivers\x64\3\Old" AND TgtFilePath CONTAINS ".dll" AND TgtFileIsSigned != "signed"
```

By excluding signed DLL's we should eliminate most false positives, so what remains would be considered suspicious files that could indicate attempts to exploit this vulnerability.

Any files found should be have their hash checked against Virus Total for further analysis.

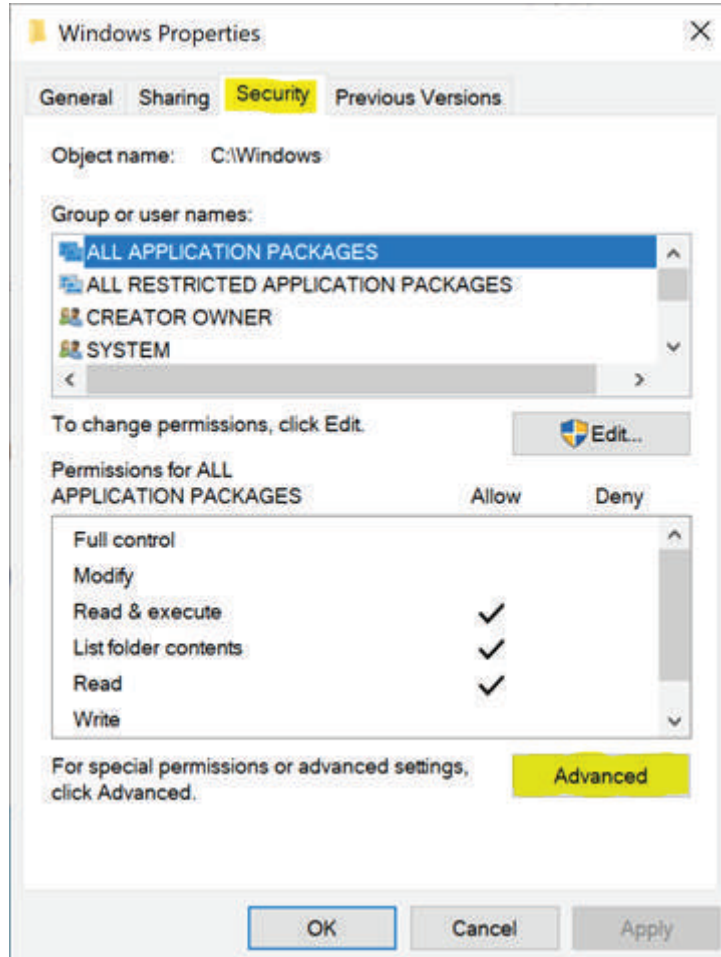


CALM

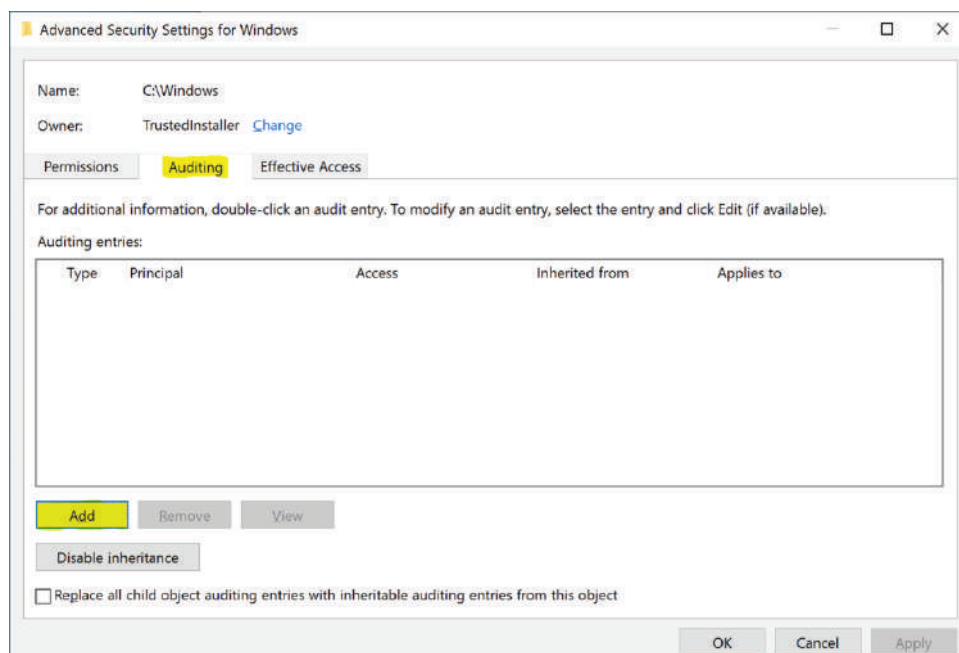
For CALM users, you'll need to have the correct Auditing policy in place, otherwise the right events wont be logged.

In particular, the file system SACL permissions need to be set to allow 4663 events to be logged.

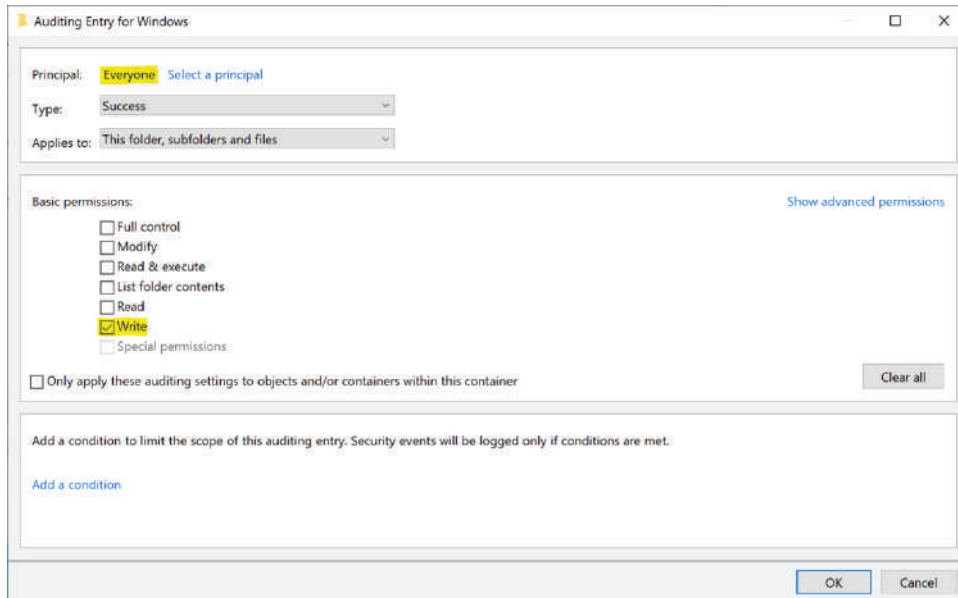
Right click on the Windows Folder and choose Properties, then select the Security tab, followed by "Advanced".



Select the Auditing tab, followed by "Add".

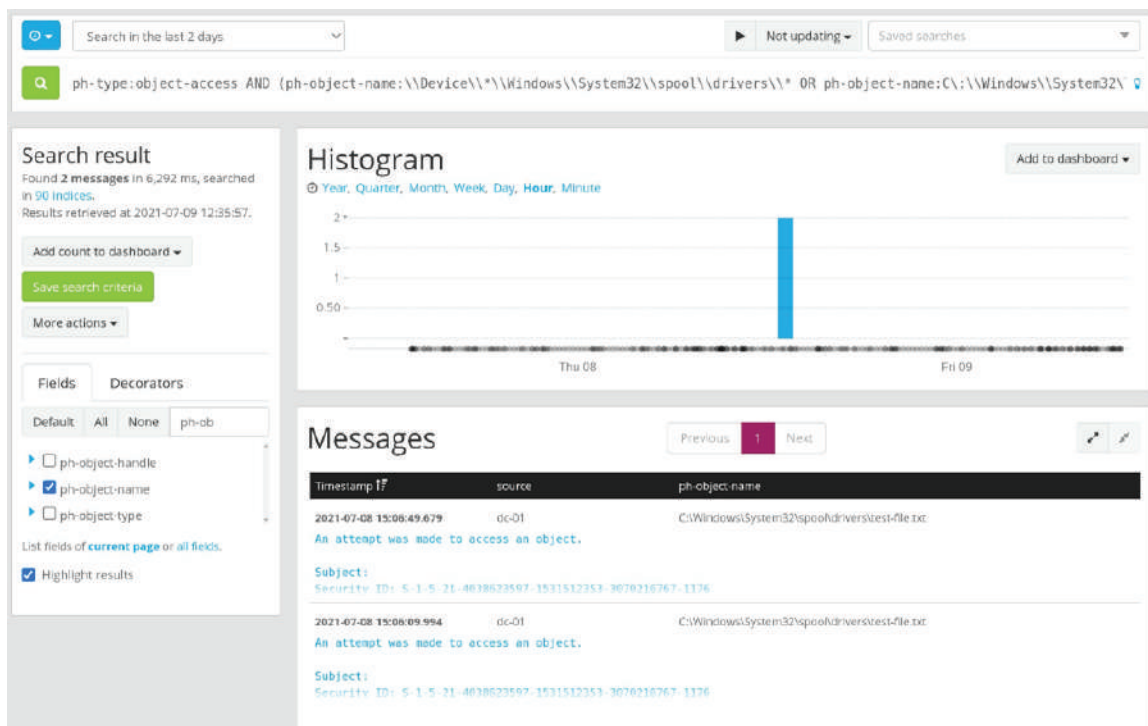


Under “Principal” select “Everyone”, and just select the Write permission and press OK



Ensure the checkbox “Replace all child object auditing entries with inheritable auditing entries from this object” is checked, and press OK.

(Note – if you have custom auditing policies for sub-directories of the Windows folder enabled, then this will replace them. If you need a more bespoke auditing policy then please configure it accordingly, this is just a guide).



Once this is enabled, you will then be able to search CALM for any writes to any files within the C:\Windows directory, but the above search query in CALM will identify any DLL's that have been uploaded to:

ph-type:object-access AND (ph-object-name:\\Device*\\Windows\\System32\\spool\\drivers* OR ph-object-name:C:\\Windows\\System32\\spool\\drivers*) AND (ph-perms-requested:6 OR ph-perms-requested:2)

DATA LAKE

As with CALM above, you will need to ensure the correct auditing policy is in place before you'll get any meaningful logs in Datalake.

If you have sysmon installed in your environment, you can also make use of the following search queries:

NAME	DESCRIPTION	SEARCH CONDITIONS
Detect for abnormal DLL loaded via sysmon 11 (File Create)	This will help to detect any new DLLs loaded by spool driver	<code>event_code = 11image_name = spoolsv.exeTargetFileName = \System32\spool\drivers\x64\3*</code>
Abnormal Parent-child relationship for spool service	Detect cmd, powershell as the parent process for spoolservice	<code>Event_code = 4688 or 1 (if you are searching in sysmon logs)process_name = spoolsv.exe parent_process_name = cmd.exe or powershell.exe user = NT AUTHORITY\System</code>
Failed Spooler logs	Need to enable Microsoft print logs (printservice/operation log via GPO) to check for any failed attempt to load the DLLs Enable 808 log	Default file names used in PoC exploitation myexploit.dll, evil.dll, addcube.dll, rev.dll, rev2.dll, main64.dll, mimilib.dll <code>Event_code = 808</code>
Abnormal image loaded to the driver	Change sysmon config to enable logging by adding this line in sysmon config file - <code><ImageLoaded name="technique_id=1210,technique_name=Exploitation of Remote Services" condition="begin with">C:\Windows\System32\spool\drivers\</ImageLoaded></code>	<code>Event_code = 7 ImageLoaded C:\Windows\System32\spool\drivers*</code> Additionally, you can check for any unsigned DLLs loaded via event ID 7 for spool service <code>Signed = False Image = Spoolsv.exe</code>
Detect abnormal registry changes for persistence via sysmon	Check when spoolsv.exe changes the registry values	<code>Event_code = 13HKLM\System\CurrentControlSet\Control\Print\Environments\Windows x64\Drivers\Version-*\<config-file>TargetObject=HKLM\System\CurrentControlSet\Control\Print\Environments\Windows x64\Drivers\Version-*\<new dll file></code> ** Highlighted ones are the new entries



Email: sales@cybanetix.com



LinkedIn: www.linkedin.com/company/cybanetix



Website: www.cybanetix.com



Contact number: 02083967442