

Project final ReporT

CVE-2021-1675

ICT287 Computer Security



Thien Twee Zian

34664971

Submission Date:

**Table of Contents**

[Introduction 2](#_Toc141451328)

[Objective of Demonstration 2](#_Toc141451329)

[Tools Required for Demonstration 3](#_Toc141451330)

[Exploitation Demonstration 4](#_Toc141451331)

[Understanding the Exploit 9](#_Toc141451332)

[Mitigation 10](#_Toc141451333)

[Conclusion 11](#_Toc141451334)

[Appendix 12](#_Toc141451335)

[Vulnerability Details : CVE-2021-1675 (Details 2022) 12](#_Toc141451336)

[Remote Procedure Call (RPC) in Operating System 13](#_Toc141451337)

[Flowchart to indicate the exploitability of PrintNightmare across various platform configurations (Dormann 2021) 14](#_Toc141451338)

[References 15](#_Toc141451339)

# Introduction

CVE-2021-1675, also called PrintNightmare, is an Elevation of Privilege Vulnerability that specifically focuses on the Windows Print Spooler application activated by default on all Windows-based systems. Exploiting this vulnerability enables an attacker with limited access privileges to construct and employ a malicious DLL file, which by doing so, the attacker can execute an exploit and attain elevated privileges.

CVE-2021-1675, also referred to by the same name, resembles CVE-2021-34527. Nevertheless, they differ in terms of their nature. While 1675 is categorized as a privilege elevation vulnerability, 34527 is classified as a remote code execution (RCE) vulnerability. In the context of this report, our focus will solely be on CVE-2021-1675.

In this report, we would look into how would the vulnerability be exploited, the steps to take, a description on how the exploit works, and the expected outcome to be achieved.

# Objective of Demonstration

In this demonstration, we will be using the script to create an account in the target system with administrative rights from an ordinary account, which is not possible in a normal setting, taking advantage of the Windows Print Spooler vulnerability (CVE-2021-1675).

At the end of the demonstration, we would gain access to the system using an administrative account. From there, we would have gained unlimited privileges, thus showcasing the elevation of privilege from the ordinary account.

**Tools Required for Demonstration**

For the demonstration of exploiting CVE-2021-1675, we would use the following tools,

|  |  |
| --- | --- |
| **Name** | **Description** |
| Windows 10 x64 Operating System (OS) | Version build 1909, with admin and user accounts set up |
| Windows Powershell | PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. It is built in default with every Windows OS. |
| PrintNightmare Script | Script to be run in powershell on target, credits to Caleb Stewart and John Hammond, taken from GitHub. |

In the demonstration, we would be using a Windows 10 OS, which is set up specifically for this test. The admin and user accounts are created, with the usernames and password as “admin” and “user” respectively. The Windows Print Spooler application is left operating, which is as per its original default.

A copy of the necessary tools can be found in the link below:

<https://murdochuniversity-my.sharepoint.com/:f:/r/personal/34664971_student_murdoch_edu_au/Documents/ICT287%20Final%20Report%20(Test%20Environments)?csf=1&web=1&e=AjoDWl>

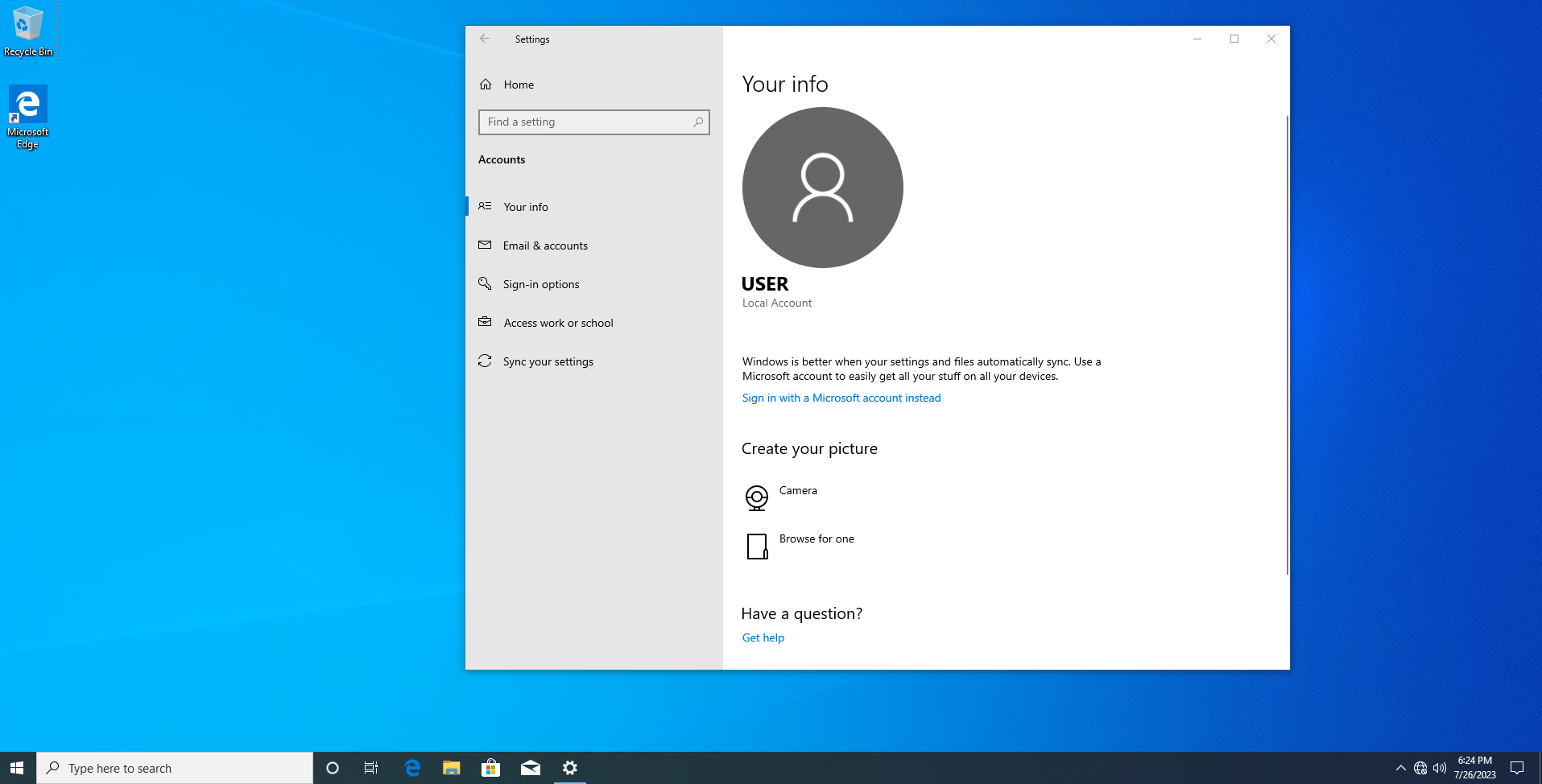
A list of vulnerability Windows versions are listed in the appendix, taken from [www.cvedetails.com](http://www.cvedetails.com).

# Exploitation Demonstration

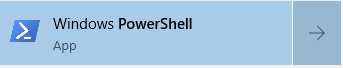
Using the tools listed in the demonstration, we will be showing how to exploit the CVE-2021-1675 from the target system.

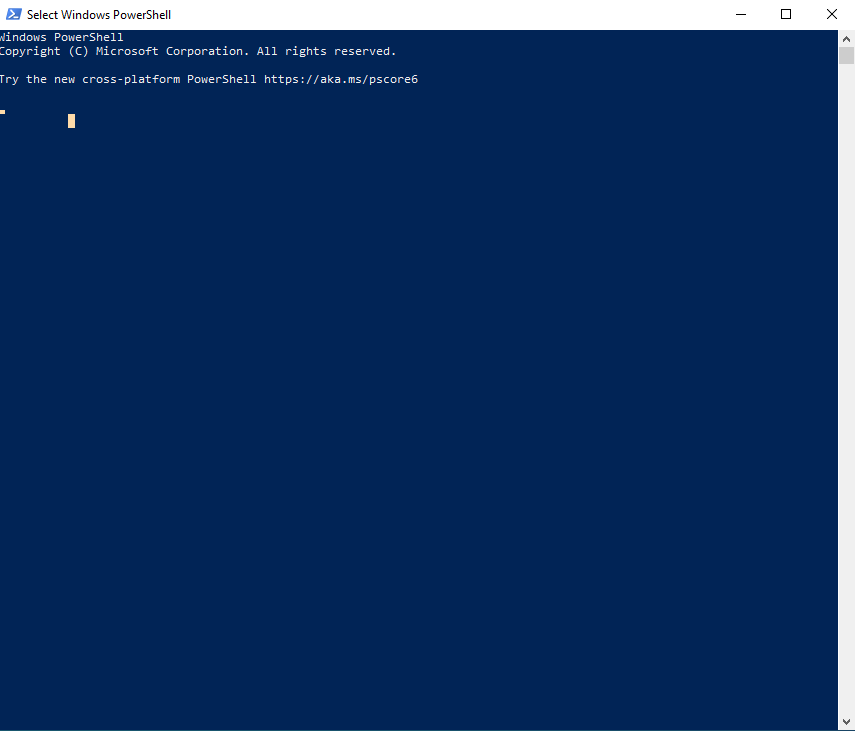
The premise is of anyone with access to the vulnerable Windows system running the Print Spooler application, together with access to the PowerShell, would be open to the exploit. Important to note is the ease of running this exploit, which would also serve to highlight the dangers of this vulnerability, as anyone with no prior background in hacking would be able to carry out this form of exploitation.

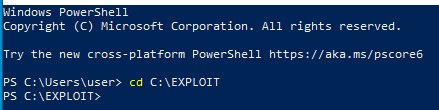
To begin, we will open the target system and access the user account to simulate an ordinary user of the system.



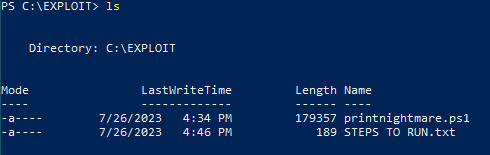
In this demonstration, we have included the script in C:\EXPLOIT. The script does not necessarily have to be located as per mentioned, but it is required to take note of the location for accessing it in the PowerShell.

We now open the PowerShell application on the target system, which can be done using the search function on the windows for easier access.  


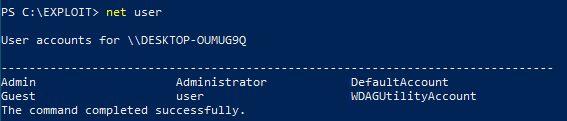


Once in, we would traverse into the folder containing the script, which in this case is C:\EXPLOIT, using the cd command. 

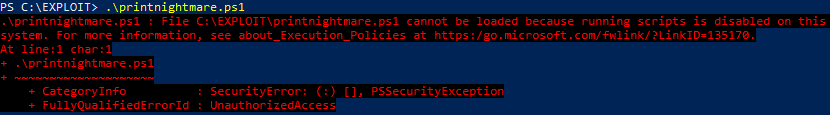
Once in, we can verify the existence of the script using the ls command.



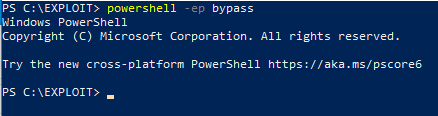
Before running the script, we can use the net user command to check the account names in the system currently, which in this case is as follows,



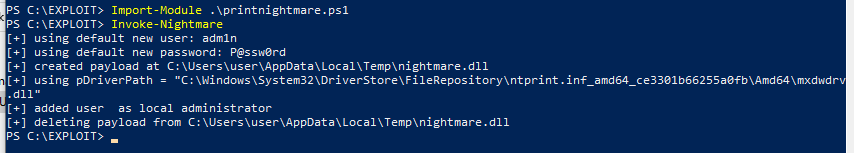
We will now run our script in the folder, named printnightmare.ps1. Before doing so, we must allow running scripts to be enabled, else the following error would occur,



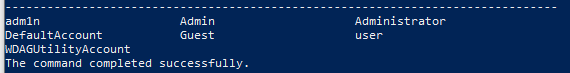
We can do so by using the command powershell -ep bypass.



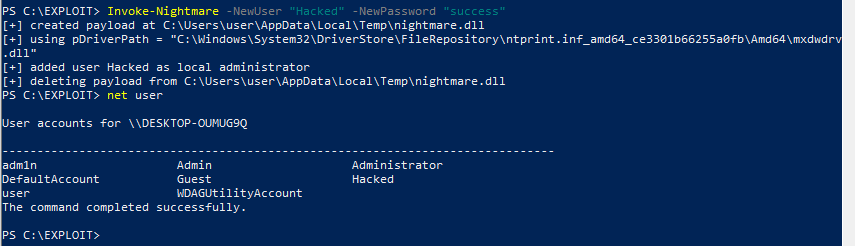
We will run the script using Import-Module "path to file", which in this case it would be Import-Module printnightmare.ps1. Once done, we can run the function within using Invoke-Nightmare. Once done, the following lines would be displayed,



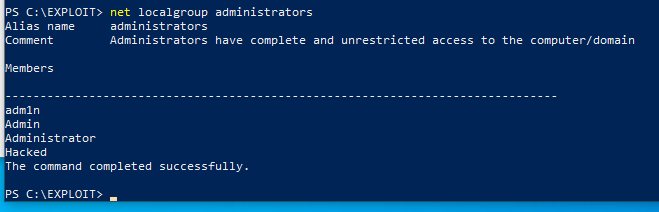
An admin account has been created with the username adm1n, and password of P@ssword. We can now run the net user command again to check if the admin account is created.



We can also use the function to create an admin account with our own username and password. For example, to create an account with the username Hacked and password success, we would use the following command Invoke-Nightmare -NewUser "Hacked" -NewPassword "success". We would check again for if the account is added successfully using net user.



We can also use the net localgroup administrators command to find out if the accounts created has administrator rights.



From this, we can see that the original account, Admin, is listed together with the two other accounts created in this example, adm1n & Hacked. This would therefore prove that our exploitation was carried out successfully, and elevation of privilege was achieved from the ordinary account user.

# Understanding the Exploit

The CVE-2021-1675 works primarily on the RpcAddPrinterDriver call of the Windows Print Spooler application, which is a remote procedure call (RPC). More on RPC can be found in the appendix. The call is used to add a driver printer into the system, storing the desired driver in a local directory.

According to the Kaspersky site CVE-2021-1675 (https://securelist.com/quick-look-at-cve-2021-1675-cve-2021-34527-aka-printnightmare/103123/), when using the call, the system has to provide multiple parameters to the Print Spooler service:

* pDataFile – a path to a data file for this printer;
* pConfigFile – a path to a configuration file for this printer;
* pDriverPath – a path to a driver file that’s used by this printer while it’s working.

The service makes several checks to ensure pDataFile and pDriverPath are not Universal Naming Convention (UNC) paths, which is the naming system applied in Microsoft Windows, but there is no corresponding check for pConfigFile, meaning the service will copy the configuration DLL to the folder %SYSTEMROOT%\system32\spool\drivers\x64\3\ (on x64 versions of the OS).

Now, if the Windows Print Spooler service tries to add a printer again, but this time sets pDataFile to the copied DLL path (from the previous step), the print service will load this DLL because its path is not a UNC path, and the check will be successfully passed. These methods can be used by a low-privileged account, and the DLL is loaded by the NT AUTHORITY\SYSTEM group process.

From this, we can understand that due to how the RpcAddPrinterDriver call is coded, the checks in place for the pDataFile can easily be circumvented by

1. Loading the malicious DLL file path to the pConfigFile
2. Manipulating the path for pDataFile to pConfigFile.

Using this exploit, any users in the system can execute a malicious DLL file with SYSTEM privileges. From this, in our example we shown to have successfully executed a DLL file with creates a new administrator account. The script provided would also be able to execute any DLL files the attacker wishes to run, using the command Invoke-Nightmare -DLL "path to file".

A flowchart on the exploitability of PrintNightmare across various platform configurations can be found in the appendix.

# Mitigation

In Microsoft’s security guidelines, users of the affected Windows operating system should install the security update KB5004945, which addresses the issue. According to the update, after installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system’s Trusted Root Certification Authorities trusts signed drivers.

Another method to ensure better security is to disable the Print Spooler service if it is not required. This can be done using the following commands on PowerShell

Stop-Service -Name Spooler -Force

Set-Service -Name Spooler -StartupType Disabled

By doing so, it would disable the ability to print both locally and remotely, therefore users have to ensure that this service is not necessary in their usage before implementing this fix.

# Conclusion

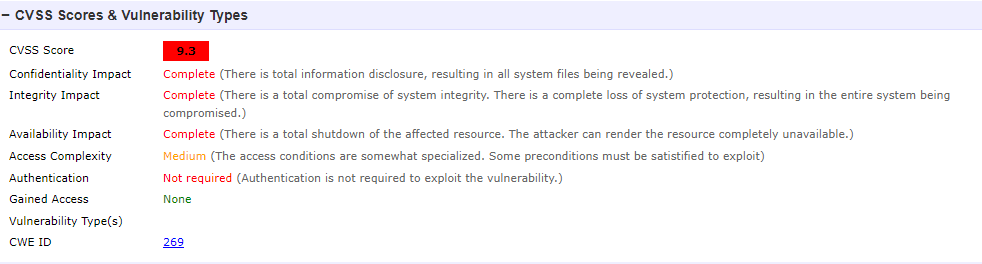
From this demonstration report associated with CVE-2021-1675, it becomes evident that vulnerabilities can be present even in default applications provided by major companies like Windows. This underscores the significance of regular updates to counter the ever-increasing occurrence of vulnerabilities in the wild.

Furthermore, understanding the ease with which this vulnerability can be exploited, coupled with the availability of accessible tools on the internet for novice users to learn and employ, emphasizes the importance of maintaining constant vigilance against such threats. It is crucial to recognize that these threats can originate from various sources, including disgruntled employees within an organization who may lack prior experience but possess the intention to cause harm.

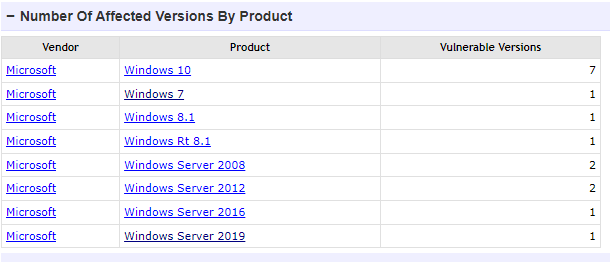
# Appendix

## Vulnerability Details : CVE-2021-1675 (Details 2022)

From <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2021-1675>



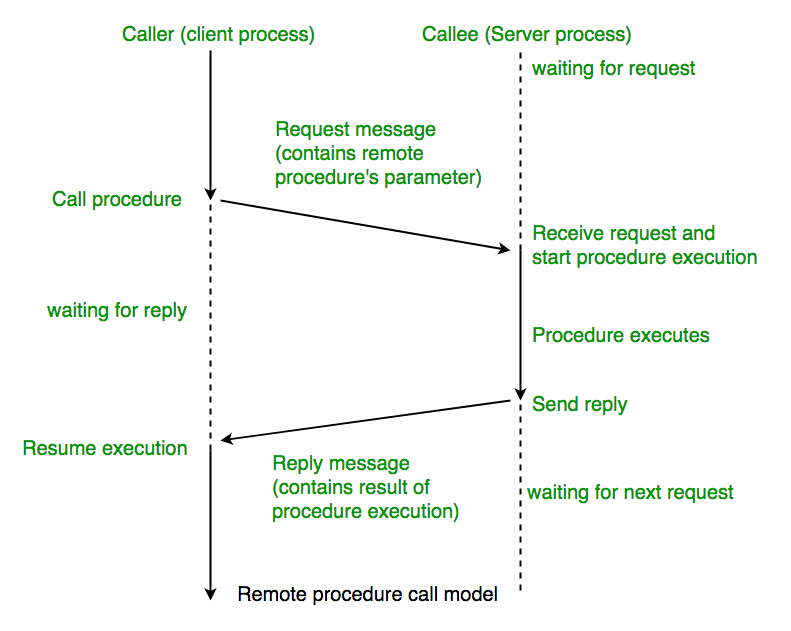




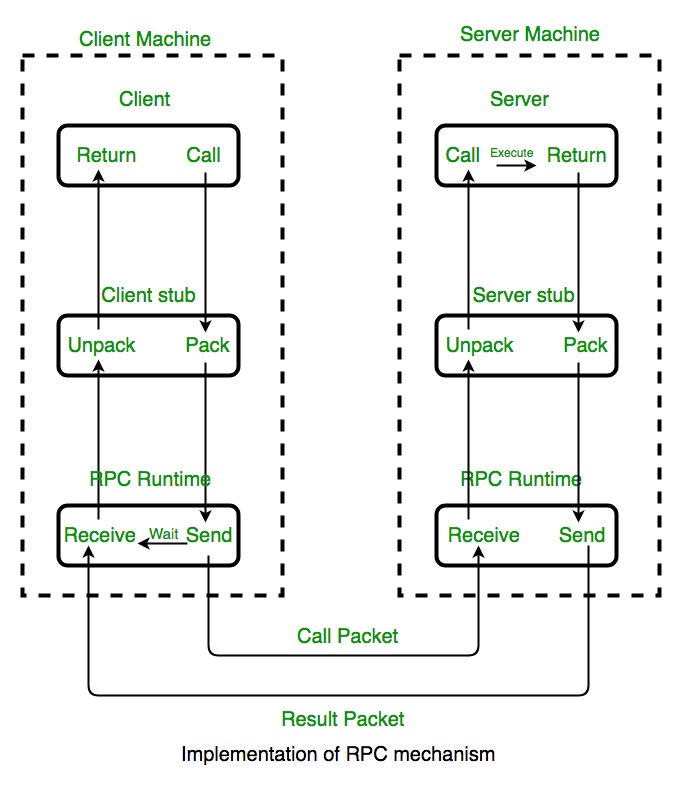
## Remote Procedure Call (RPC) in Operating System

From <https://www.geeksforgeeks.org/remote-procedure-call-rpc-in-operating-system/>

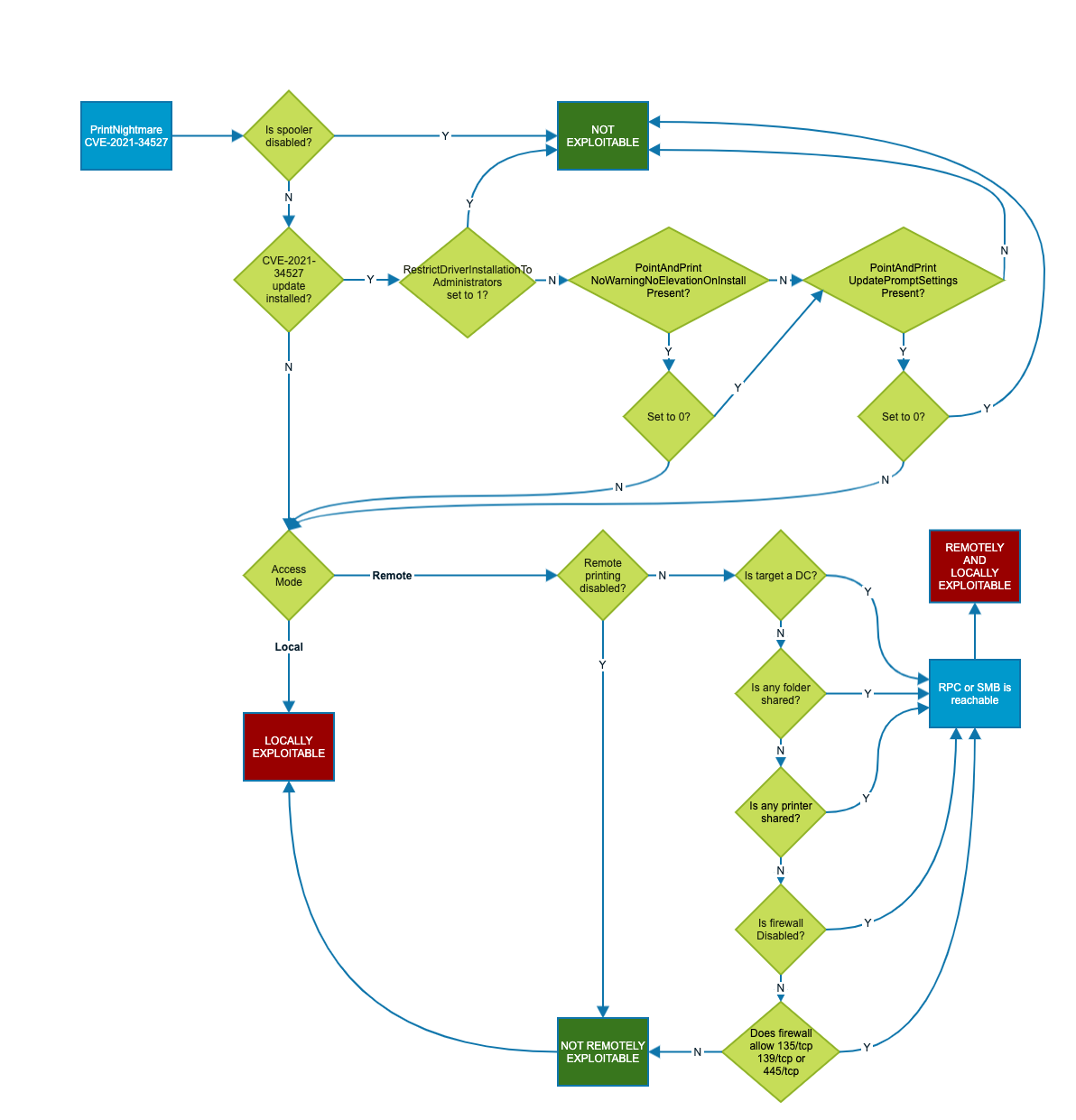
When making a Remote Procedure Call:



Working of RPC



## Flowchart to indicate the exploitability of PrintNightmare across various platform configurations (Dormann 2021)



# References

Details, C. (2022). "Windows Print Spooler Elevation of Privilege Vulnerability." from <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2021-1675>.

Dormann, W. (2021). "Microsoft Windows Print Spooler allows for RCE via AddPrinterDriverEx()." from <https://www.kb.cert.org/vuls/id/383432>.

Lab, K. (2021). "Quick look at CVE-2021-1675 & CVE-2021-34527 (aka PrintNightmare)." from <https://securelist.com/quick-look-at-cve-2021-1675-cve-2021-34527-aka-printnightmare/103123/>.

Lab, K. (2021). "A Windows Print Spooler vulnerability called PrintNightmare."

Laskowski, B. (2021). "PrintNightmare (CVE-2021-1675 and CVE 2021-34527) Explained." from <www.blumira.com/cve-2021-1675/>.

Microsoft (2021). "July 6, 2021—KB5004945 (OS Builds 19041.1083, 19042.1083, and 19043.1083) Out-of-band." from <https://support.microsoft.com/en-us/topic/july-6-2021-kb5004945-os-builds-19041-1083-19042-1083-and-19043-1083-out-of-band-44b34928-0a71-4473-aa22-ecf3b83eed0e>.

Microsoft (2021). "KB5005010: Restricting installation of new printer drivers after applying the July 6, 2021 updates." from <https://support.microsoft.com/en-us/topic/kb5005010-restricting-installation-of-new-printer-drivers-after-applying-the-july-6-2021-updates-31b91c02-05bc-4ada-a7ea-183b129578a7>.

Microsoft (2023). "Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527)." from <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>.

MiniTool (2022). "What Is Print Spooler and How to Reset It on Windows 10? [MiniTool Wiki]."

MiniTool (2023). "[Review] What Is UNC Path and How to Use It? [MiniTool Wiki]." from <https://www.minitool.com/lib/unc-path.html>.

Rapid7 (2021). "CVE-2021-34527 (PrintNightmare): What You Need to Know." from <https://www.rapid7.com/blog/post/2021/06/30/cve-2021-1675-printnightmare-patch-does-not-remediate-vulnerability/>.

Shodan (2022). "Shodan Search on Windows OS." from <https://www.shodan.io/search?query=os%3A%22windows%22>.

Singla, Y. (2023). "Remote Procedure Call (RPC) in Operating System." from <https://www.geeksforgeeks.org/remote-procedure-call-rpc-in-operating-system/>.

Stewart, C. and J. Hammond (2021). "CVE-2021-1675 - PrintNightmare LPE (PowerShell) ". from <https://github.com/calebstewart/CVE-2021-1675>.

Technology, N. I. o. S. a. (2022). "CVE-2021-1675 Detail." from <https://nvd.nist.gov/vuln/detail/CVE-2021-1675>.

Tills, C. (2021). "CVE-2021-1675: Proof-of-Concept Leaked for Critical Windows Print Spooler Vulnerability." from <https://www.tenable.com/blog/cve-2021-1675-proof-of-concept-leaked-for-critical-windows-print-spooler-vulnerability>.