Sign in

calebstewart / CVE-2021-1675 Public

Notifications Fork 230 Star 1k

Code Issues 6 Pull requests 1 Actions Projects Security Insights

main Go to file Code

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

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

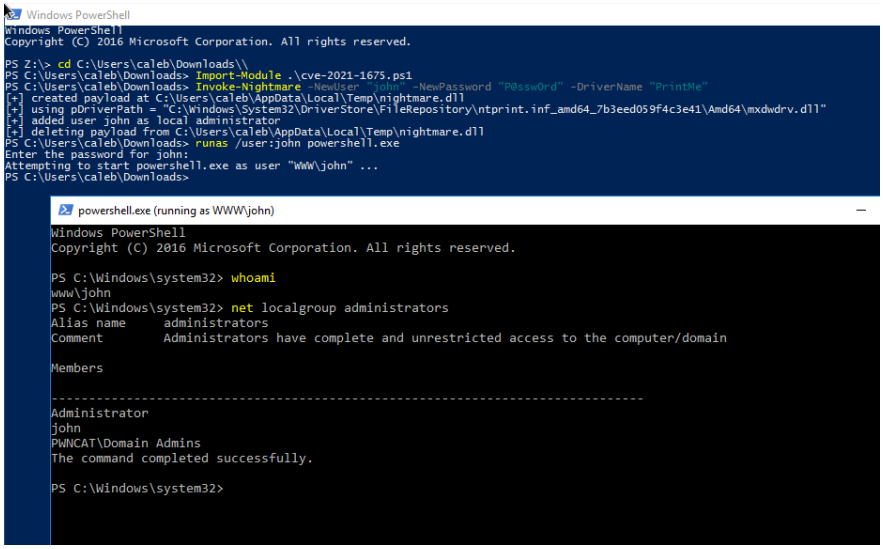
JohnHammond John Hammond

calebstewart Caleb Stewart

Languages

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.



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

Usage

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

```
Import-Module .\cve-2021-1675.ps1
Invoke-Nightmare # add user `adm1n`/`P@ssw0rd` :

Invoke-Nightmare -DriverName "Xerox" -NewUser ":
```

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
```

Details

PowerShell 99.0% Other 1.0%

- 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.

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information

© 2024 GitHub, Inc.