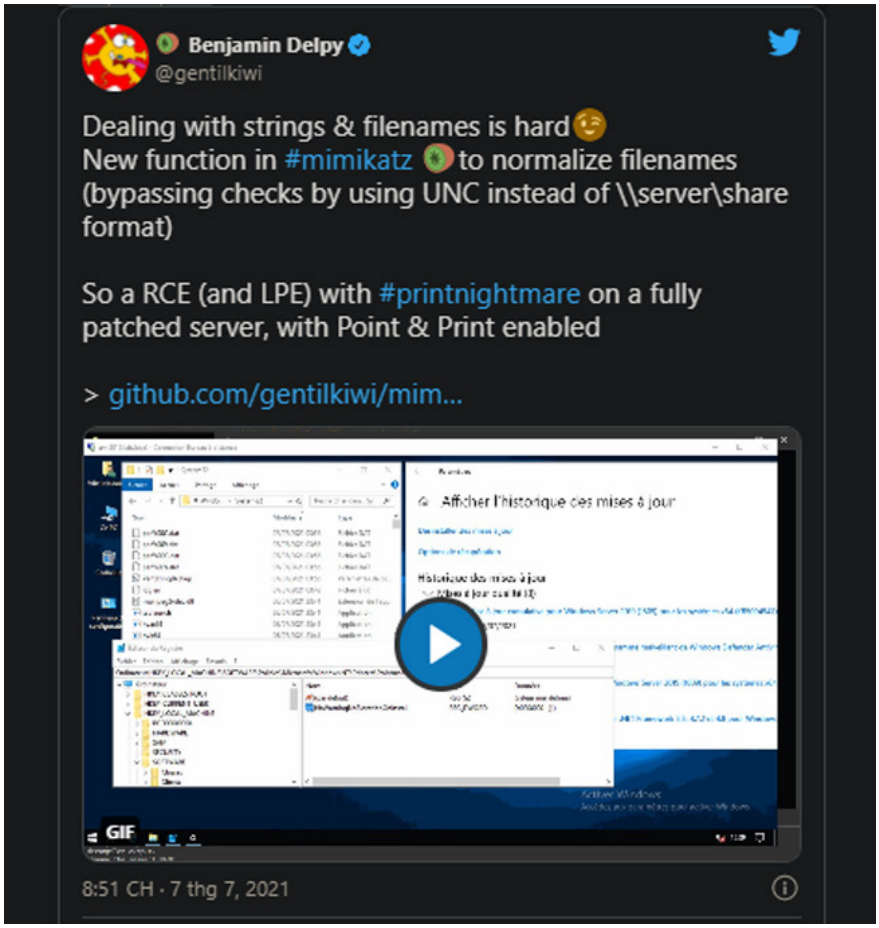
PrintNightMare vulnerability patch is flawed, attackers can still 'break through'

Yesterday, Microsoft released a patch for the PrintNightMare zero-day vulnerability. This bug allows attackers to remotely execute code on fully patched Print Spooler devices.

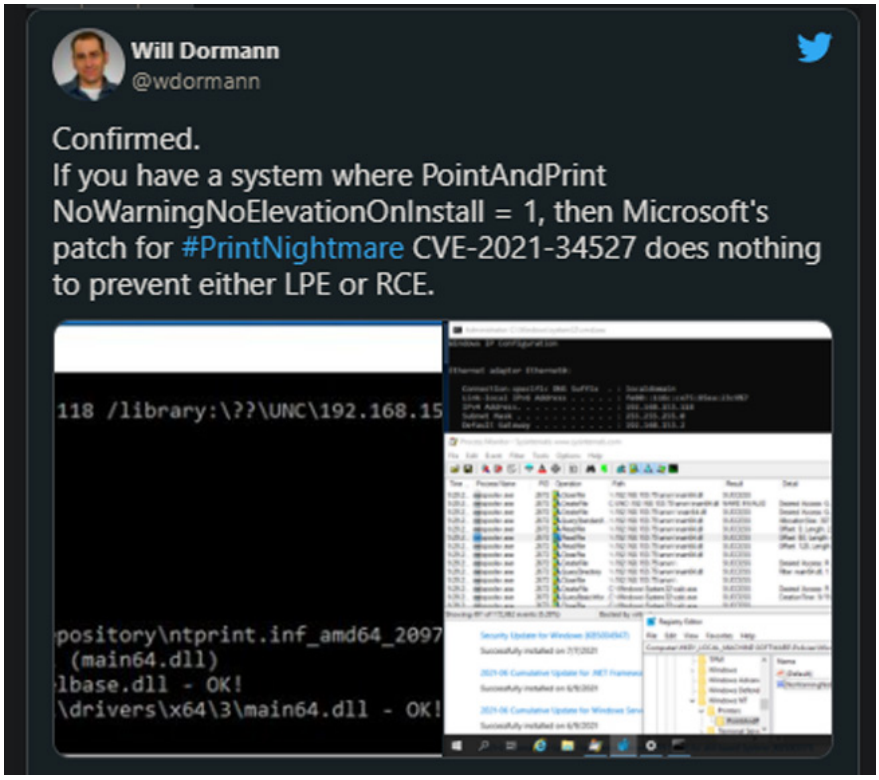
However, this urgently released patch still exposes flaws.

Microsoft only fixed the remote code exploit, which means the vulnerability can still be used for local privilege escalation (LPE). In addition, hackers soon discovered that this vulnerability could still be exploited remotely.

According to Mimikatz expert Benjamin Delpy, hackers can bypass the patch to gain SYSTEM permissions if the Point and Print policy is enabled.



This has been confirmed by Will Dorman, CERT/CC vulnerability analyst.



To bypass the PrintNightmare patch and achieve RCE and LPE, the 'Point and Print Restrictions' policy must be enabled and the 'When installing drivers for a new connection' setting configured to 'Do not show warning on elevation prompt'.

Currently, security researchers recommend that administrators disable the Print Spooler service until all problems are completely fixed or block remote printing to the machine through Group Policy.

You can follow these steps to disable the Print Spooler service through PowerShell:

1. Open PowerShell as Administrator
2. Stop-Service -Name Spooler -Force
3. Set-Service -Name Spooler -StartupType Disabled

Alternatively, you can send to remote printing to the machine via Group Policy by performing the following steps:

1. Open Group Policy Editor
2. Go to Computer Configuration/ Administrative Templates/ Printers
3. Disable the 'Allow Print Spooler to accept client connections:' policy

Microsoft has updated the MSRC listing to note that it is rolling out patches for Windows Server 2012, Windows Server 2016 and Windows 10, Version 1607. The company adds that for system security, users "must verify get the below registry setting set to 0 or undefined'.

HKEY_LOCAL_MACHINESOFTWAREPoliciesMicrosoftWindows NTPrinters PointAndPrint

NoWarningNoElevationOnInstall = 0 (DWORD) or undefined (default install)

NoWarningNoElevationOnUpdate = 0 (DWORD) or undefined (default setting)

However, Dormann argued that 'NoWaringNoElevationOnInstall=0 did not prevent the exploit. The company also has not yet addressed the reports of other security research firms.