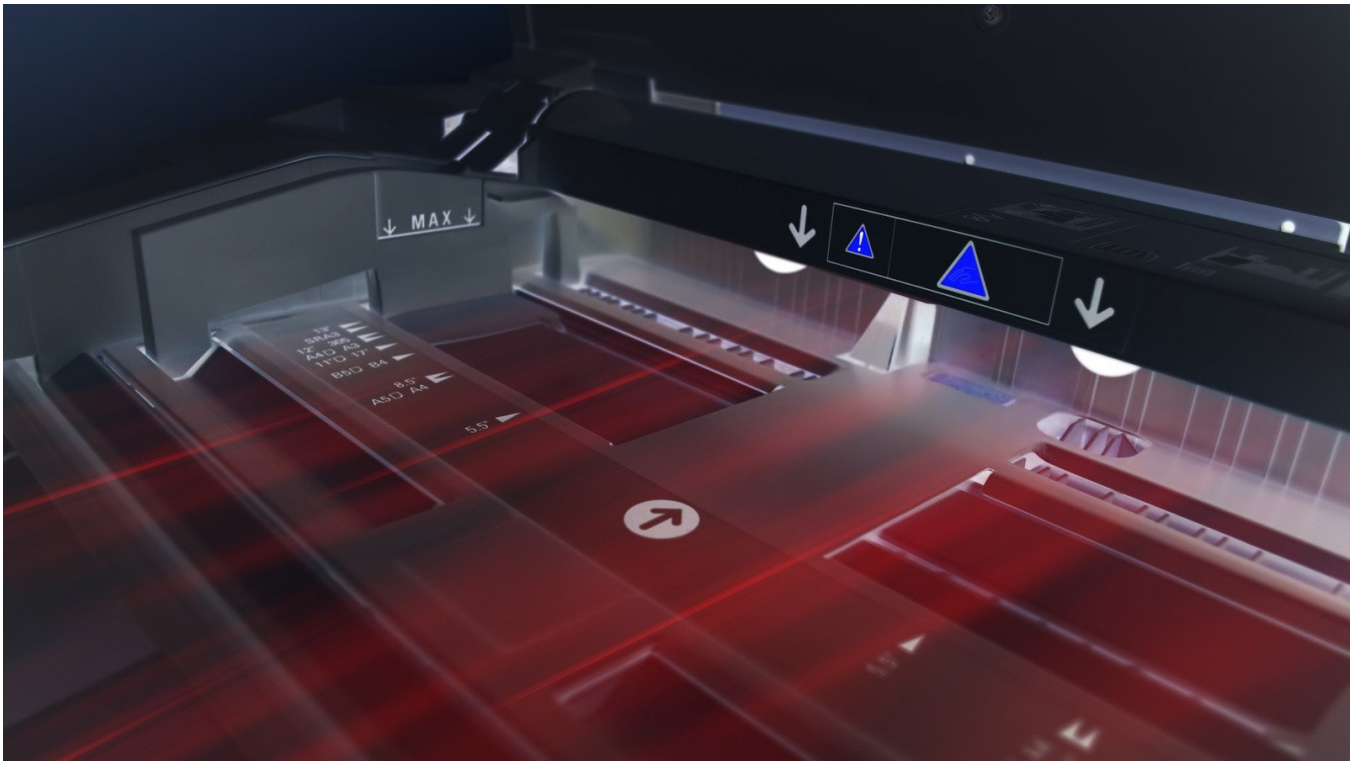
# Remote print server gives anyone Windows admin privileges on a PC

Lawrence Abrams



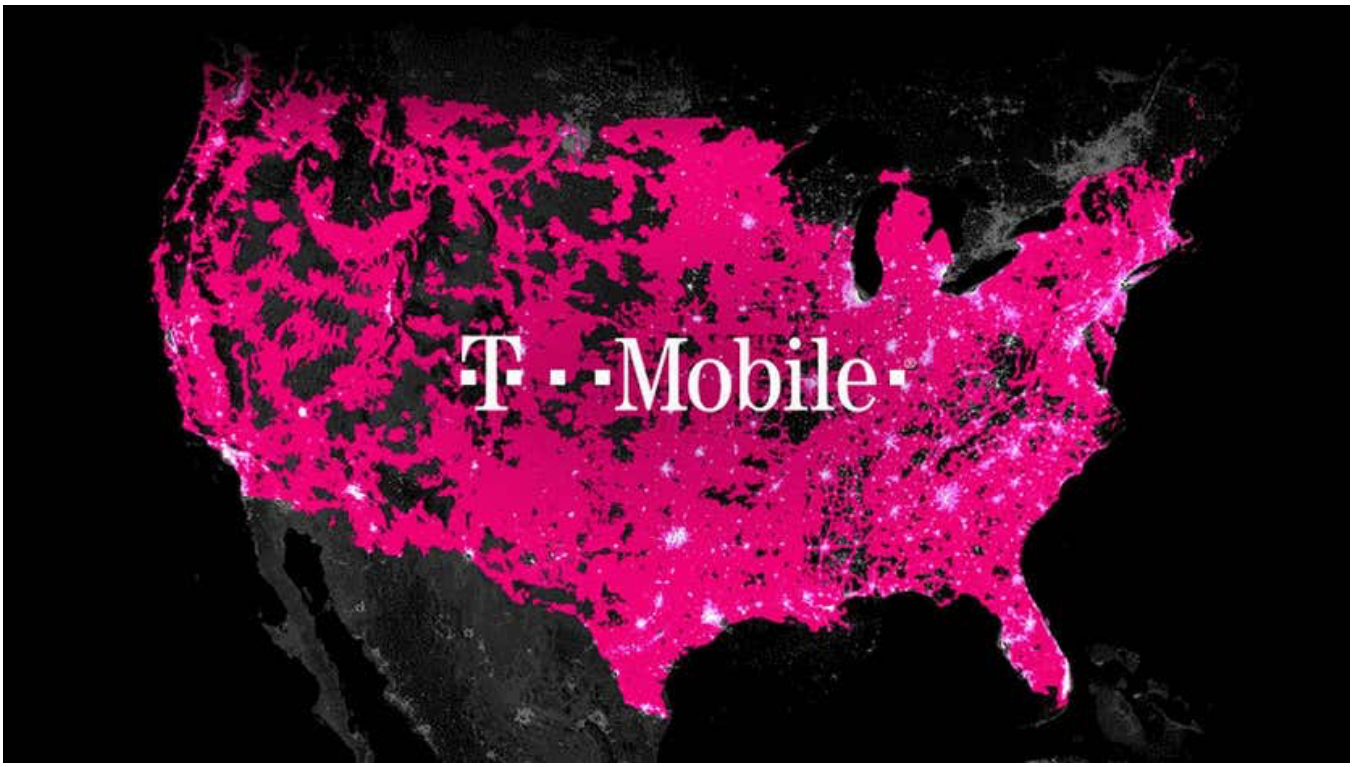

A researcher has created a remote print server allowing any Windows user with limited privileges to gain complete control over a device simply by installing a print driver.

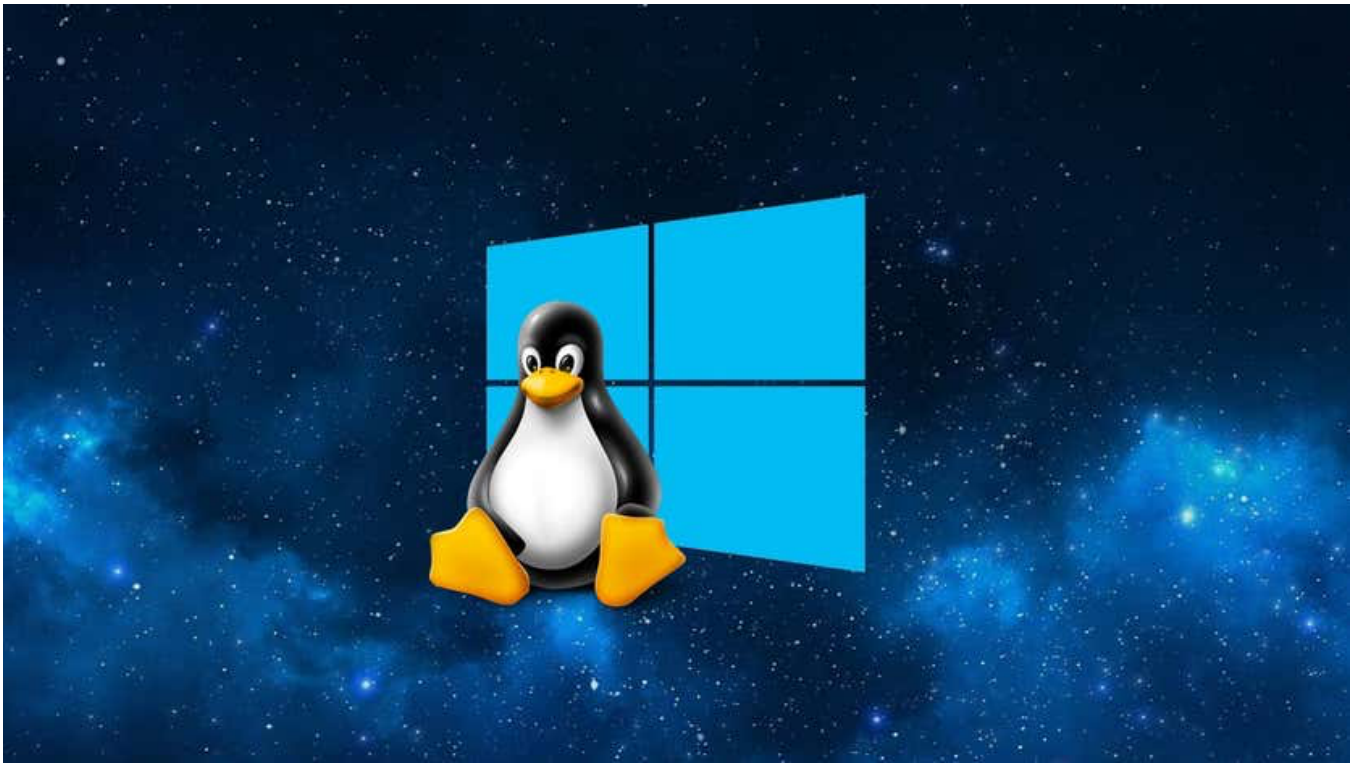
In June, a security researcher accidentally revealed a zero-day Windows print spooler vulnerability known as PrintNightmare (CVE-2021-34527) that allowed remote code execution and elevation of privileges.

While Microsoft released a security update to fix the vulnerability, researchers quickly figured out ways to bypass the patch under certain conditions.

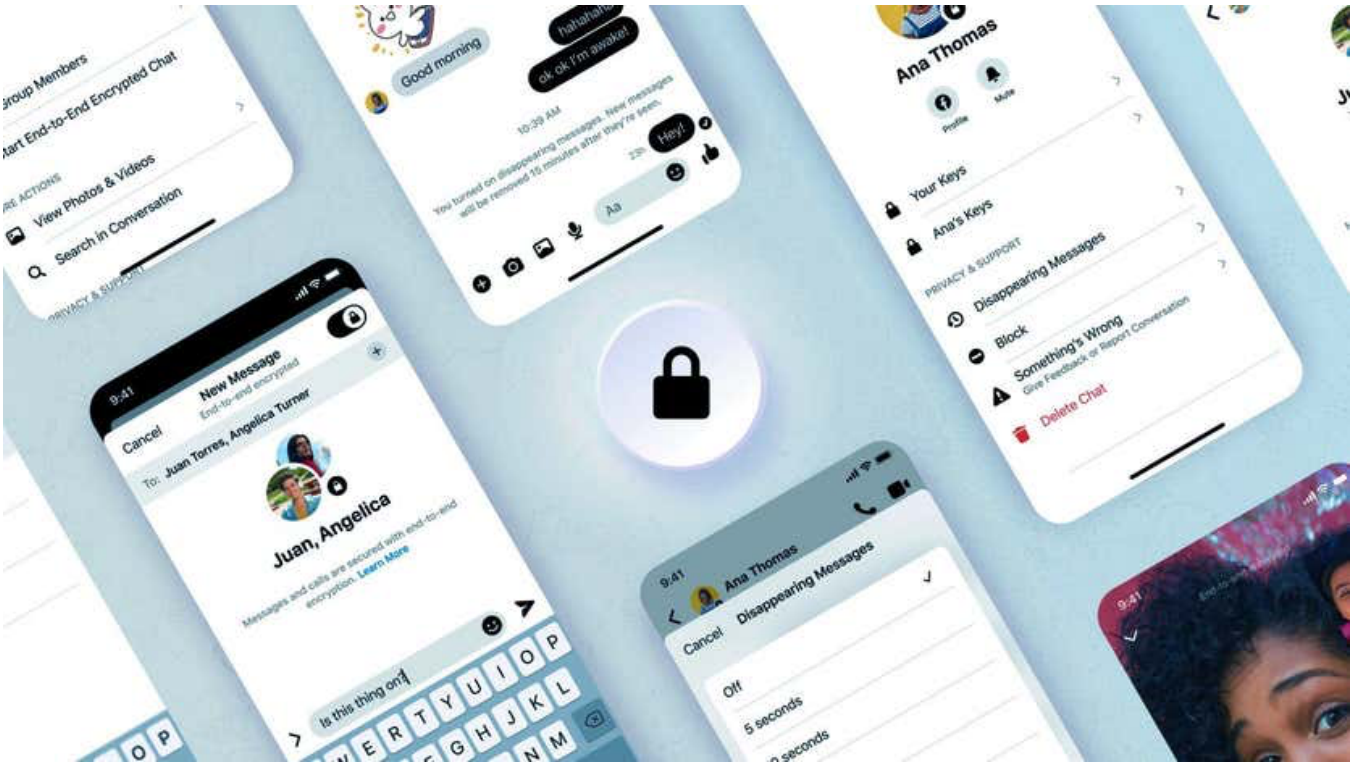
bleepingcomputer
From a bleeping computer to a working computer

## Top Articles

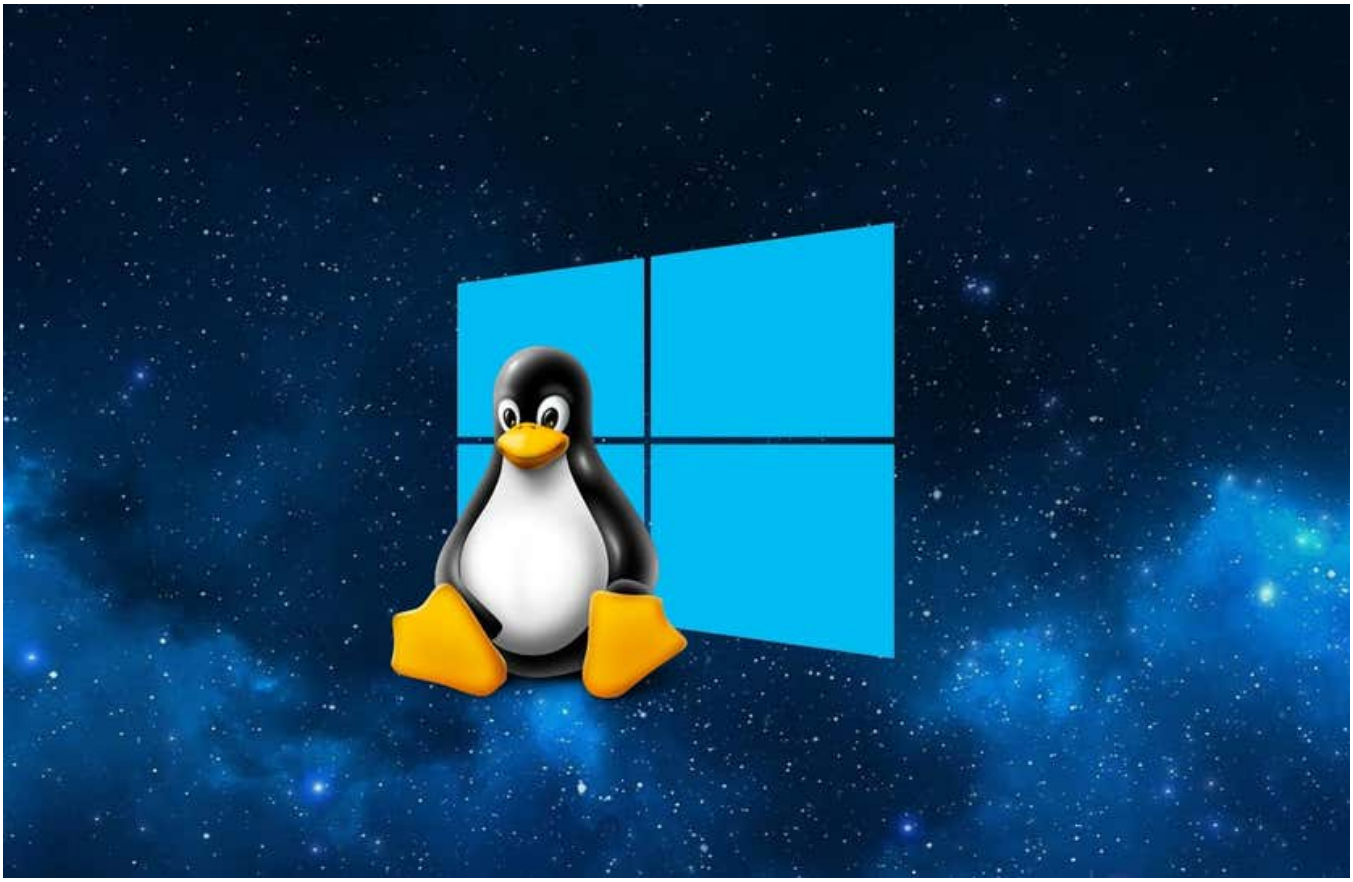




## Read More


Group Members
Start End-to-End Encrypted Chat
View Photos & Videos
Search in Conversation
Good morning
ok ok I'm awake!
Hey!
New Message
Cancel
Juan, Angelica
Is this thing on?
Ana Thomas
Your Keys
Ana's Keys
Disappearing Messages
Block
Something's Wrong
Delete Chat
Off
5 seconds

## EasyWSL turns Linux docker images into aWindows 10 WSL distro



Since then, researchers have continued to devise new ways to exploit the vulnerability, with one researcher creating an Internet-accessible print server allowing anyone to open a command prompt with administrative

privileges.

## Now anyone can get Windows SYSTEM privileges

Security researcher and Mimikatz creator Benjamin Delpy has been at the forefront of continuing PrintNightmare research, releasing multiple bypasses and updates to exploits through specially crafted printer drivers and by abusing Windows APIs.

To illustrate his research, Delpy created an Internet-accessible print server at \\printnightmare[.]gentilkiwi[.]com that installs a print driver and launches a DLL with SYSTEM privileges.

Initially, the launched DLL would write a log file to the C:\Windows\System32 folder, which should only be writable by users with elevated privileges.

As some people did not believe his initial print driver could elevate privileges, on Tuesday, Delpy modified the driver to launch a SYSTEM command prompt instead.

This new method effectively allows anyone, including threat actors, to get administrative privileges simply by installing the remote print driver. Once they gain administrative rights on the machine, they can run any command, add users, or install any software, effectively giving them complete control over the system.

This technique is especially useful for threat actors who breach networks for the deployment of ransomware as it allows quick and easy access to administrative privileges on a device that helps them spread laterally through a network.

BleepingComputer installed Delpy's print driver on a fully patched Windows 10 21H1 PC as a user with 'Standard' (limited) privileges to test this technique.

As you can see, once we installed the printer and disabled Windows Defender, which detects the malicious printer, a command prompt was opened that gave us full SYSTEM privileges on the computer.

When we asked Delpy if he was concerned that threat actors were abusing his print server, he told us that one of the driving reasons he created it is to pressure "Microsoft to make some priorities" into fixing the bug.

He also said that it's impossible to determine what IP addresses belong to researchers or threat actors. However, he has firewalled Russian IP addresses that appeared to be abusing the print servers.

Delpy has warned that this is not the end of Windows print spooler abuse, especially with new research being revealed this week at both the Black Hat and Def Con security conferences.

## Mitigating the new printer vulnerability

As anyone can abuse this remote print server on the Internet to get

SYSTEM level privileges on a Windows device, Delpy has offered several ways to mitigate the vulnerability.

These methods are outlined in a CERT advisory written by Will Dormann, a vulnerability analyst for CERT/CC.

## Option 1: Disable the Windows print spooler

The most extreme way to prevent all PrintNightmare vulnerabilities is to disable the Windows Print spooler using the following commands.

```
Stop-Service -Name Spooler -Force

Set-Service -Name Spooler -StartupType Disabled
```

However, using this mitigation will prevent the computer from being able to print.

## Option 2: Block RPC and SMB traffic at your network boundary

As Delpy's public exploit uses a remote print server, you should block all RPC Endpoint Mapper (`135/tcp`) and SMB (`139/tcp` and `445/tcp`) traffic at your network boundary.

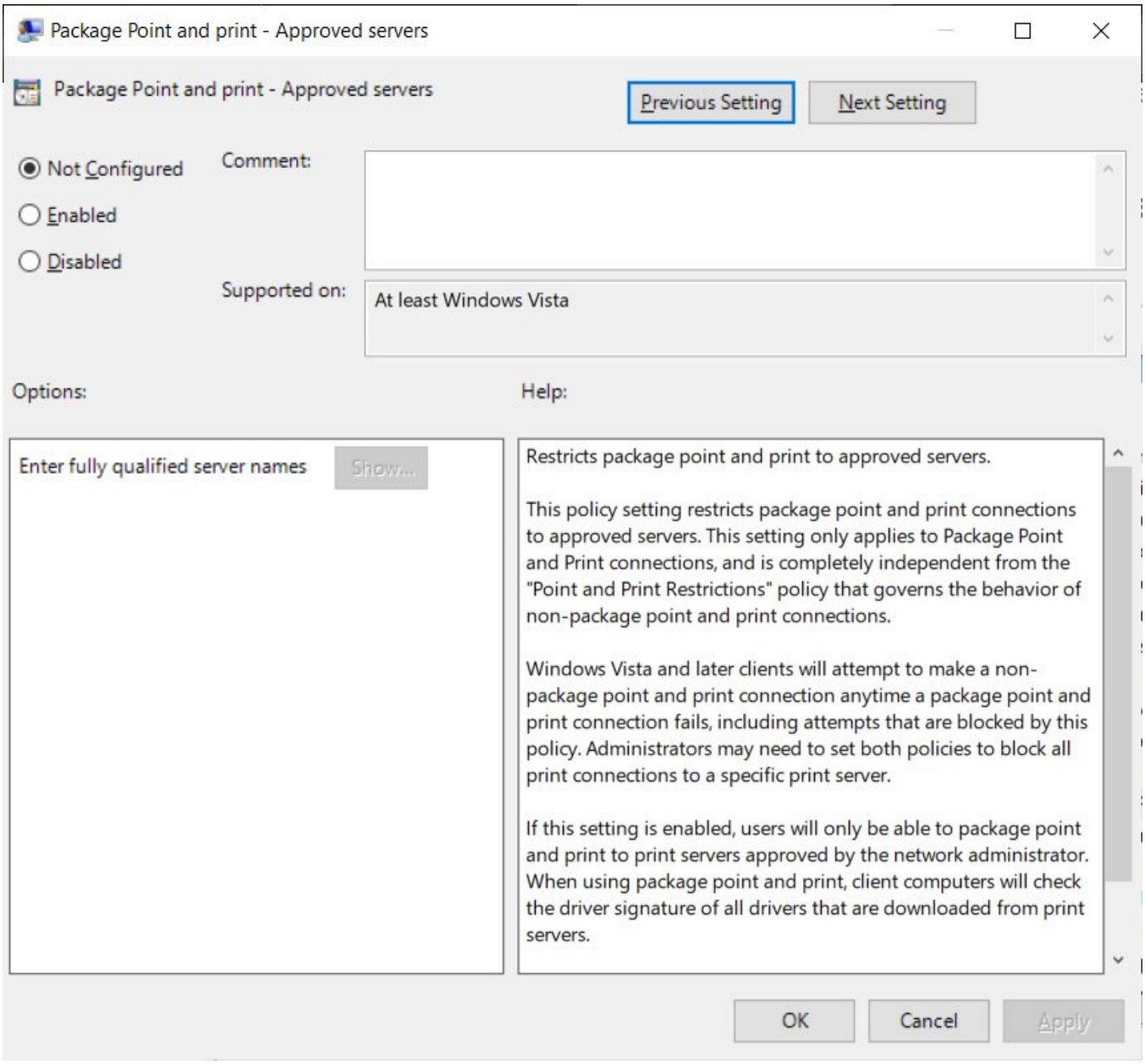
However, Dormann warns that blocking these protocols may cause existing functionality to no longer work as expected.

"Note that blocking these ports on a Windows system may prevent expected capabilities from functioning properly, especially on a system that functions as a server," explained Dormann.

## Option 3: Configure PackagePointAndPrintServerList

The best way to prevent a remote server from exploiting this vulnerability is to restrict Point and Print functionality to a list of approved servers using the 'Package Point and print - Approved servers' group policy.

This policy prevents non-administrative users from installing print drivers using Point and Print unless the print server is on the approved list.




**Package Point and print - Approved servers group policy**

To enable this policy, launch the Group Policy Editor (gpedit.msc) and navigate to **User Configuration** > **Administrative Templates** > **Control Panel** > **Printers** > **Package Point and Print – Approved Servers**.

Then enable the policy and enter the list of servers that you wish to allow to use as a print server and then press **OK** to enable the policy. If you do not have a print server on your network, you can enter a fake server name to enable the feature.

Using this group policy will provide the best protection against the known exploit but will not prevent a threat actor from taking over an allowed print server with malicious drivers.

*Update 8/1/21: Added more information about the Package Point and Print - Approved servers policy. Thx bikerdude!*

## Related Articles:

Microsoft fixes Windows Print Spooler PrintNightmare vulnerability

New Windows PrintNightmare zero-days get free unofficial patch

Windows security update KB5004945 breaks printing on Zebra printers

Microsoft's incomplete PrintNightmare patch fails to fix vulnerability

How to mitigate Print Spooler vulnerability on Windows 10