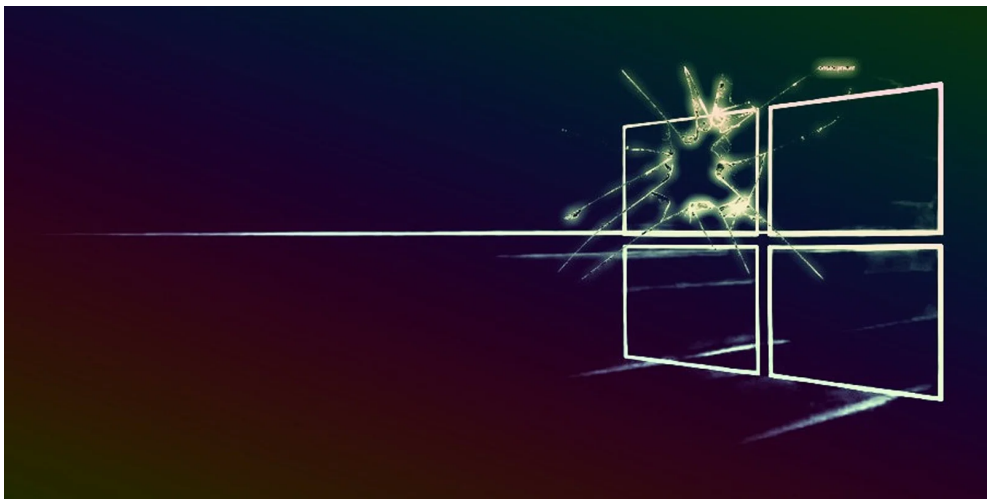
New Windows security updates break network printing

By Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/) September 16, 2021 12:08 PM 4



Windows administrators report wide-scale network printing problems after installing this week's September 2021 Patch Tuesday security updates.

On Tuesday, Microsoft released sixty security updates (https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2021-patch-tuesday-fixes-2-zero-days-60-flaws/) and fixes

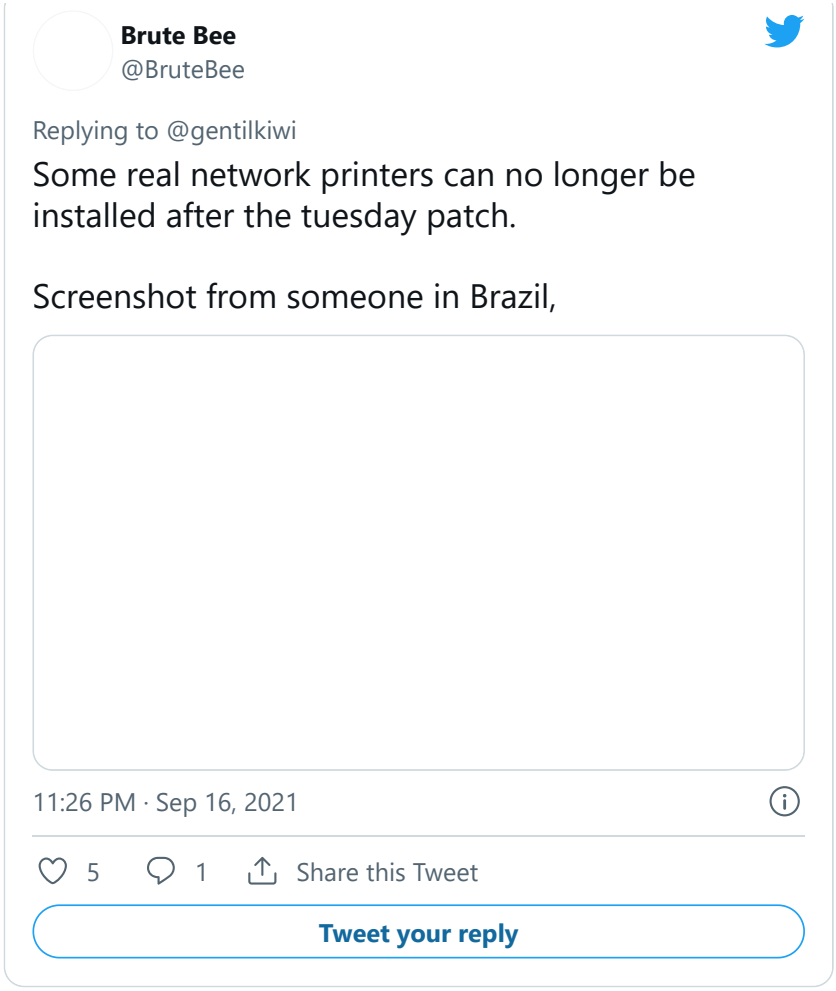
for numerous bugs as part of their monthly Patch Tuesday updates, including a fix for the last remaining PrintNightmare vulnerability (https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-remaining-windows-printnightmare-vulnerabilities/) tracked as CVE-2021-36958 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958).

This vulnerability is critical to fix as it is used by numerous ransomware gangs and threat actors to immediately gain SYSTEM privileges on vulnerable devices, as demonstrated below.

Demonstration of remote PrintNightmare driver open a SYSTEM command prompt
from BleepingComputer.com

01:49

However, many Windows system administrators are now reporting [1 (https://docs.microsoft.com/en-us/answers/questions/517533/pint-server-and-print-nightmare-update.html?page=3&pageSize=10&sort=oldest), 2 (https://www.reddit.com/r/sysadmin/comments/pochxo/microsoft_fixes_remaining_windows_printnightmare/)] that their computers can no longer print to network printers after installing the PrintNightmare fixes on their print servers.



In conversations with multiple Windows admins dealing with these issues, they all told BleepingComputer that the updates are breaking their network printing, and they can only fix them by removing the updates.

"The problem has happened for us on different sites. The print servers were 2012R2 and 2016. All worked fine before the update," one administrator told BleepingComputer.

"After yesterday's Windows Update, none of the network computers can print to Windows 10 computer we use as a print server," another admin told BleepingComputer.

"As far as i know, this affected both printers with v3 and v4 drivers, but I'm not 100% sure (this issue was different from the issue emerged with the previous update which broke v3 printers). After uninstalling the patch on the server everything got back to normal," another admin told us yesterday.

While all users are experiencing problems with network printing, they do not see the same errors.

For example, one person told us that their devices are displaying a 4098 Warning in the Application event logs. This error states, "The user" preference item in the" Group Policy Object did not apply because it failed with error code '0x8007011b' This error was suppressed."

Another admin told us that their Printer ports tab was blank, while another said they received "Access Denied" errors.

These issues also appear to be affecting all network printers, including HP, Canon, Konica Minolta, and label printers, and for both Type 3 and Type 4 printer drivers.

Those with USB printers connected directly to their computers are not having any issues.

The updates associated with the new PrintNightmare security update and the subsequent network printing problems are:

- KB5005568 (https://support.microsoft.com/en-us/topic/september-14-2021-kb5005568-os-build-17763-2183-d19b2778-204a-4c09-a0c3-23dc28d5deac) (Windows Server 2019)
- KB5005613 (https://support.microsoft.com/en-gb/topic/september-14-2021-kb5005613-monthly-rollup-47b217aa-8d33-4b29-b444-77fcbe57410b) (Windows Server 2012 R2)
- KB5005627 (https://support.microsoft.com/en-us/topic/september-14-2021-kb5005627-security-only-update-3404d598-7d6e-4007-93e8-49438460791f) (Windows Server 2012 R2)
- KB5005623 (https://support.microsoft.com/en-us/topic/september-14-2021-kb5005623-monthly-rollup-bcdb6598-517e-4d53-aa7c-dd7fcfdca204) (Windows Server 2012)
- KB5005607 (https://support.microsoft.com/en-au/topic/september-14-2021-kb5005607-security-only-update-f2cb16bb-7282-4f2e-a43e-50c4163c877c) (Windows Server 2012)
- KB5005606 (https://support.microsoft.com/en-us/topic/september-14-2021-kb5005606-monthly-rollup-e6cb2ae9-f688-4f8b-b742-43b03b791d6d) (Windows Server 2008)
- KB5005618 (https://support.microsoft.com/en-us/topic/september-14-2021-kb5005618-security-only-update-08a80048-babc-41ce-8b4b-cfd10c7c0dda) (Windows Server 2008)
- KB5005565 (https://support.microsoft.com/en-us/topic/september-14-2021-kb5005565-os-builds-19041-1237-19042-1237-and-19043-

1237-292cf8ed-f97b-4cd8-9883-32b71e3e6b44) (Windows 10 2004, 20H2, and 21H1)

- KB5005566 (https://support.microsoft.com/en-us/topic/september-14-2021-kb5005566-os-build-18363-1801-c2535eb5-9e8a-4127-a923-0c6a643bba1d) (Windows 10 1909)
- KB5005615 (https://support.microsoft.com/en-au/topic/september-14-2021-kb5005615-security-only-update-78aa3b33-a4d9-49ad-bb28-1394943a3d7b) (Windows 7 Windows Server 2008 R2)

PrintNightmare fixes causing significant problems

Unfortunately, to fix the PrintNightmare vulnerabilities, Microsoft has had to make significant changes over the past two months to the Windows Point and Print feature and how drivers can be installed from a print server.

These changes include requiring administrator privileges to install a printer driver via the Point and Print feature.

Once Microsoft made these changes, Windows users began receiving errors when trying to print, or Windows would prompt for an administrative password to update printer drivers.

While Microsoft has introduced new registry settings (https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872) that allow you to control these changes, disabling them will once again make a Windows device vulnerable.

According to security researcher Benjamin Delpy (https://twitter.com/gentilkiwi), this week's PrintNightmare fix also introduced new changes that automatically block the CopyFiles directive (https://docs.microsoft.com/en-us/windows-hardware/drivers/print/downloading-queue-specific-files) print driver feature.

Admins can configure this change via the Windows Registry **CopyFilesPolicy** value under the **HKLM\Software\Policies\Microsoft\Windows NT\Printers** key. When set to '1', CopyFiles will be enabled again.

If other printer drivers are used in your organization that uses the CopyFiles directive, they will no longer work, leading to further conflicts.

BleepingComputer has contacted Microsoft with questions about these issues but has not heard back at this time.