**Security Advisory 2021-033**

# Vulnerabilities in Microsoft Print Spooler

***September 17, 2021 — v1.7***

**TLP:WHITE**

*History:*

- *30/06/2021 — v1.0 – Initial publication*
- *01/07/2021 — v1.1 – Update with information about issues with the patch*
- *02/07/2021 — v1.2 – Update with information about new vulnerability*
- *07/07/2021 — v1.3 – Update with information about new patch*
- *08/07/2021 — v1.4 – Update with information about issues with the new patch*
- *16/07/2021 — v1.5 – Update with information about a third vulnerability*
- *13/08/2021 — v1.6 – Update with information about a fourth vulnerability and updates*
- *17/09/2021 — v1.7 – Update with information about new patch*

## Summary

On the 8th of June 2021, Microsoft – as part of the Patch Tuesday release – has issued updates that addressed multiple vulnerabilities including the Windows Print Spooler Remote Code Execution Vulnerability CVE-2021-1675 with CVSS score 7.8. This vulnerability was initially rated as a low-importance elevation-of-privilege vulnerability, but on the 21st of June Microsoft reviewed the issue and labeled it as a remote code execution flaw [1]. Proof-of-concept exploit code for the CVE-2021-1675 flaw has been published online, the flaw impacts the Windows Print Spooler service and could be exploited to compromise Windows systems ([2] the Github page is not available anymore). On the 30th of June 2021, further analysis proved that the exploit - nicknamed *PrintNightmare* - still works on a fully patched domain controller or systems that have the Point and Print configured with the `NoWarningNoElevationOnInstall` option configured [3].

On the 2nd of July 2021, Microsoft announced a second vulnerability – CVE-2021-34527 – related to PrintNightmare remote code execution. This vulnerability is similar, but distinct from the vulnerability that is assigned CVE-2021-1675. On the 6th of July 2021, Microsoft released an update for several versions of Windows to address this new vulnerability. Updates are not yet available for Windows 10 version 1607, Windows Server 2016, or Windows Server 2012. On the 7th of July 2021, Microsoft released the updates for Windows Server 2012, Windows Server 2016 and Windows 10, Version 1607 versions [5].

On the 14th of July 2021, Microsoft announced a third vulnerability: CVE-2021-34481 with a CVSS base score of 7.8. The researcher who discovered this flaw does not consider it to be a variant of PrintNightmare [7]. Nevertheless it is also related to Microsoft Print Spooler.

Despite the updates provided by Microsoft in July, various security researchers still found pos-

sibilities to exploit the Point and Print feature to install malicious print drivers that allowed low-privileged users to gain SYSTEM privileges in Windows. [9]

On the 10th of August, Microsoft released new updates that fix CVE-2021-34481 [10]. These updates, and later ones, will require, by default, administrative privilege to install drivers.

On the 11th of August, Microsoft updated the CVSS score of the CVE-2021-34481 from 7.8 to 8.8 [8]. Microsoft discovered a remote path to exploit this vulnerability that was, at first, local. On the same day, Microsoft issued an advisory about this a vulnerability named CVE-2021-36958 [11].

As part of September 2021 Patch Tuesday, Microsoft has released a new security update that fixes CVE-2021-36958 [12]. However, networking printing problems were reported from the community after deploying the patches [14].

## Technical Details

Exploitation of CVE-2021-1675 could give remote attackers full control of vulnerable systems. To achieve RCE, attackers would need to target a user authenticated to the spooler service. Without authentication, the flaw could be exploited to elevate privileges, making this vulnerability a valuable link in an attack chain.

The vulnerability resides in the authentication process of `RpcAddPrinterDriver`. A normal user can bypass this authentication and install a malicious driver in the print server. In a domain, a normal domain user can connect to the Spooler service in the domain controller and install a driver into the DC. Then, he can execute code as `SYSTEM` on the domain controller and fully control the Domain.

As per CVE-2021-34527 the vulnerability is in the same function, `RpcAddPrinterDriverEx` and an attack must involve an authenticated user. The remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with `SYSTEM` privileges. An attacker could then install programs; view, change, delete data; or create new accounts with full user rights.

For CVE-2021-34527, Microsoft advised about additional settings that should be checked in order to secure the system. The *Point and Print* registry settings are not directly related to this vulnerability, but this technology weakens the local security posture in such a way that exploitation will still be possible [5]. More details on how to mitigate this can be found in the Recommendations section.

CVE-2021-34481, when exploited, allows for local privilege escalation to the level of SYSTEM and an attacker could then install programs, view, change, delete data or create new accounts with full user rights. To exploit this vulnerability an attacker must have the ability to execute code on a victim system. However, on the 11th of August, Microsoft discovered a remote path to exploit this vulnerability.

The CVE-2021-36958 vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations [12]. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, delete data; or create new accounts with full user rights. While Microsoft classifies this vulnerability as Remote Code Execution, the attack needs to be performed locally, according to researchers [11].

## Affected Products

- Windows Server 2016
- Windows Server 2019
- Windows Server 2012 (including R2)
- Windows Server 2008 (including R2, R2 SP1 and R2 SP2)
- Windows 7, 8.1 and 10 (including versions 1909)
- Windows Server, version 2004
- Windows Server, version 20H2

## Recommendations

**Apply the patches as soon as possible.** CVE-2021-1675 was fully patched as part of Microsoft's Patch Tuesday release on June 8, 2021 [1], and CVE-2021-34527 was patched with a security patch that can be found on the vendor's advisory site [5]. The CVE-2021-34481 was patched as part of Microsoft Patch Tuesday release on August 10, 2021 [8].

Finally, in September 2021 Patch Tuesday security updates, Microsoft has released a new security update for CVE-2021-36958 that fixes the remaining PrintNightmare vulnerability [13]. However, Windows administrators report wide-scale network printing problems [14]. Testing before deploying the last patches should be taken into consideration especially for the following updates:

- KB5005568 (Windows Server 2019)
- KB5005613 (Windows Server 2012 R2)
- KB5005627 (Windows Server 2012 R2)
- KB5005623 (Windows Server 2012)
- KB5005607 (Windows Server 2012)
- KB5005606 (Windows Server 2008)
- KB5005618 (Windows Server 2008)
- KB5005565 (Windows 10 2004, 20H2, and 21H1)
- KB5005566 (Windows 10 1909)
- KB5005615 (Windows 7 Windows Server 2008 R2)

**Additionally**, for CVE-2021-34527, it must be confirmed that the following registry settings are set to `0` (zero) or are not defined [5]:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
```

- `NoWarningNoElevationOnInstall = 0 (DWORD)` or not defined (default setting)
- `NoWarningNoElevationOnUpdate = 0 (DWORD)` or not defined (default setting)

**Note:** Having `NoWarningNoElevationOnInstall` set to `1` makes your system vulnerable by design. These registry keys do not exist by default, and therefore are already at the secure setting.

**Optionally**, configure the `RestrictDriverInstallationToAdministrators` registry value to prevent non-administrators from installing printer drivers on a print server. Therefore, after the Microsoft update for CVE-2021-34527 is installed, a registry value called `RestrictDriverInstallationToAdministrators` in the key:

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint\
```

should be checked. It is intended to restrict printer driver installation to only administrator users. Please see KB5005010 for more details [6].

### Mitigation

In case the patches cannot be applied, the workaround is to disable the Spooler service [5]. It is described how to do it on both GPO and PowerShell in [4]. This should be done after a careful analysis of the impact.

Another option is to disable inbound remote printing through Group Policy. These settings can also be configured via Group Policy as follows:

- *Computer Configuration / Administrative Templates / Printers*
- Disable the *Allow Print Spooler to accept client connections* policy to block remote attacks.

The impact of this workaround is that this policy will block the remote attack vector by preventing inbound remote printing operations. The system will no longer function as a print server, but local printing to a directly attached device will still be possible [5].

Regarding CVE-2021-36958, Microsoft recommends disabling the Print Spooler [12] - this will disable the ability to print both locally and remotely. However, other "non-official" mitigations exist that do not involve disabling the Print Spooler. It consists in allowing devices to install printers only from authorised servers [11]. This can be set up via Group Policy as follows:

- *User Configuration / Administrative Templates / Control Panel > Printers / Package Point and Print – Approved Servers.*
- Then, enter the list of allowed print servers. If there is no print server on the network, a fake server can be set to enable the feature.

Using this group policy will provide the best protection against CVE-2021-36958 exploits but will not prevent threat actors from taking over an authorised print server with malicious drivers.

## References


[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675

[2] https://github.com/afwu/PrintNightmare (not available anymore)

[3] https://www.kb.cert.org/vuls/id/383432

[4] https://github.com/LaresLLC/CVE-2021-1675

[5] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

[6] https://support.microsoft.com/en-us/topic/kb5005010-restricting-installation-of-new-printer-drivers-after-applying-the-july-6-2021-updates-31b91c02-05bc-4ada-a7ea-183b129578a7

[7] https://twitter.com/Junior_Baines

[8] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481

[9] https://www.bleepingcomputer.com/news/microsoft/windows-print-nightmare-continues-with-malicious-driver-packages/

[10] 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

[11] https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-another-windows-print-spooler-zero-day-bug/

[12] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958

[13] https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-remaining-windows-printnightmare-vulnerabilities/

[14] https://www.bleepingcomputer.com/news/security/new-windows-security-updates-break-network-printing/