A part of the **Department of the Environment, Climate & Communications**



# NCSC Alert

---

## Microsoft Windows Print Spooler RCE Vulnerability - CVE-2021-34527 UPDATE
## 2021-07-09

**Status:** TLP-WHITE

## Revision History

| Revision | Date | Author(s) | Description |
|---|---|---|---|
| 1.0 | 01 July 2021 | CSIRT-IE | Initial Alert created regarding new Print Spooler Vulnerability affecting Microsoft Windows. |
| 1.1 | 02 July 2021 | CSIRT-IE | Additional information from Microsoft, including the assignment of CVE-2021-34527 and link to Microsoft guidance |
| 1.2 | 07 July 2021 | CSIRT-IE | Updated to include details about patch released by Microsoft |
| 1.3 | 09 July 2021 | CSIRT-IE | Clarified guidance added from Microsoft regarding additional measures that are required to secure environments |

# 1 Vulnerability Details

| | |
|---|---|
| **Threat Type** | The NCSC are aware of a Remote Code Execution (RCE) vulnerability, along with Proof of Concept (PoC) code for the Microsoft Windows Print Spooler service **(CVE-2021-34527)**. This vulnerability can allow an authenticated, remote attacker to gain SYSTEM privileges by sending an RpcAddPrinterDriverEx() RPC request in all versions of Windows. <br><br> The RpcAddPrinterDriverEx() function is used to install a printer driver on a system. Any authenticated user can call RpcAddPrinterDriverEx() loading a driver file locally or from a remote system. By leveraging the vulnerability, the Print Spooler Service, spoolsv.exe, executes code in an arbitrary DLL file with SYSTEM privileges. <br><br> CSIRT-IE strongly recommend that all organisations examine the **Security Update Guide** from Microsoft and apply appropriate mitigations where neccessary. Microsoft has also released **clarified guidance** regarding the effectiveness of the security update and questions around the suggested mitigations |
| **Products Affected** | All versions of Microsoft Windows |
| **Impact** | Remote Code Execution - compromised systems, data loss. |
| **Recommendations** | Microsoft released a patch on 6th July 2021. Please refer to the Microsoft guidance regarding this vulnerability. <br> Microsoft has recommended that customers follow these steps immediately: <br><br> • In ALL cases, apply the CVE-2021-34527 security update. The update will not change existing registry settings <br><br> • After applying the security update, review the registry settings documented in the CVE-2021-34527 advisory <br><br> • If the registry keys documented do not exist, no further action is required <br><br> • If the registry keys documented exist, in order to secure your system, you must confirm that the following registry keys are set to 0 (zero) or are not present: <br><br>    – HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint <br><br>    – NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting) <br><br>    – UpdatePromptSettings = 0 (DWORD) or not defined (default setting) |

**Recommendations contd.**
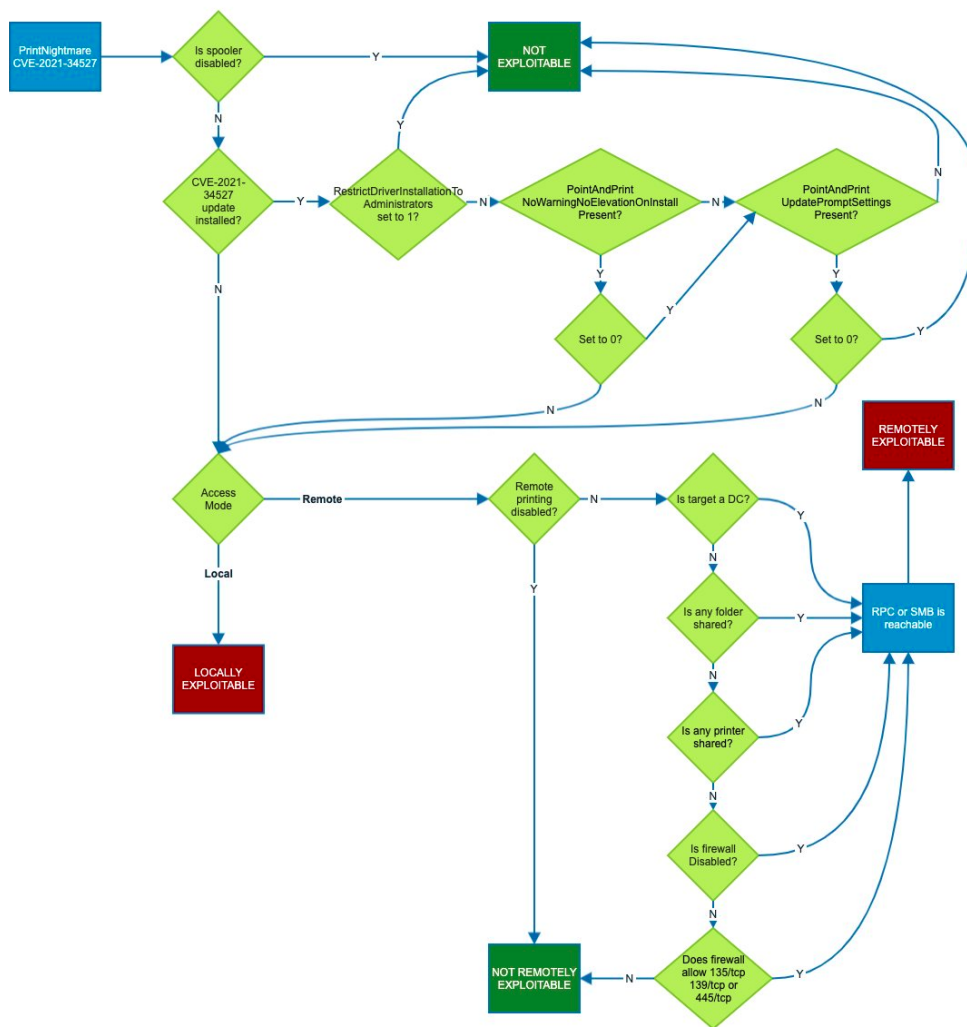


Microsoft has also provided workarounds in case the patch cannot be applied. (**Please Note:** these workarounds will need to be evaluated before being applied to your environment.):

- Disable the Print Spooler service to prevent exploitation. (Disabling the Print Spooler service disables the ability to print both locally and remotely).
- Disable inbound remote printing through Group Policy. Computer Configuration / Administrative Templates / Printers, **Disable** the **"Allow Print Spooler to accept client connections:"** policy to block remote attacks.

---

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

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
**Tel:** +353 (0)1 6782333
**Mail:** certreport@decc.gov.ie
**Web:** ncsc.gov.ie
**Twitter:** ncsc_gov_ie