# Recent vulnerabilities in Windows Print Spooler service

Microsoft has released the KB5004948 emergency security update to address the Windows Print Spooler PrintNightmare vulnerability on all editions of Windows 10 1607 and Windows Server 2016.

"An update has now been released for all affected versions of Windows that are still in support," Microsoft said in the Windows message center.

The PrintNightmare bug tracked as CVE-2021-34527 enables attackers to take over affected servers via remote code execution (RCE) with SYSTEM privileges.

Detailed steps on how to install these out-of-band security updates are available in the support documents linked below:

- Windows 10, version 21H1 (KB5004945)
- Windows 10, version 20H1 (KB5004945)
- Windows 10, version 2004 (KB5004945)
- Windows 10, version 1909 (KB5004946)
- Windows 10, version 1809 and Windows Server 2019 (KB5004947)
- Windows 10, version 1803 (KB5004949)
- Windows 10, version 1607 and Windows Server 2016 (KB5004948)
- Windows 10, version 1507 (KB5004950)
- Windows Server 2012 (Monthly Rollup KB5004956 / Security only KB5004960)
- Windows 8.1 and Windows Server 2012 R2 (Monthly Rollup KB5004954 / Security only KB5004958)
- Windows 7 SP1 and Windows Server 2008 R2 SP1 (Monthly Rollup KB5004953 / Security only KB5004951)

- Windows Server 2008 SP2 (Monthly Rollup KB5004955 / Security only KB5004959)

Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role, the company added.

You also have the option to configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server.

### Microsoft's PrintNightmare security patch is incomplete

While Microsoft says this security updates address the PrintNightmare vulnerability, security researchers have discovered that the patch is incomplete and it can be bypassed to achieve both remote code execution and local privilege escalation with the official fix installed.

However, 0patch has released free PrintNightmare micropatches on Friday that can sucessfully block attempts to exploit the vulnerability.

Windows users and admins are recommended to do one of the following until a working patch from Microsoft is released:

- Do not install the July 6th patch and install 0Patch's micropatches instead.
- Disable the Print Spooler

### Recommendations:

Option 1 - Disable the Print Spooler service on Windows

Option 2 - Disable inbound remote printing through Group Policy

CISA has also issued a notification on the PrintNightmare zero-day encouraging admins to disable the Windows Print Spooler service on servers not used for printing.

### References:

https://www.bleepingcomputer.com/news/security/microsoft-printnightmare-now-patched-on-all-windows-versions/

https://securelist.com/quick-look-at-cve-2021-1675-cve-2021-34527-aka-printnightmare/103123/

https://www.bleepingcomputer.com/news/security/cisa-disable-windows-print-spooler-on-servers-not-used-for-printing/

https://www.bleepingcomputer.com/news/security/public-windows-printnightmare-0-day-exploit-allows-domain-takeover/

https://www.bleepingcomputer.com/news/security/microsoft-pushes-emergency-update-for-windows-printnightmare-zero-day/