

Advisory for Windows Print Spooler Vulnerability

A. Description:

A highly critical vulnerability known as 'PrintNightmare' has been reported to affect Windows Operating System (both desktop and server editions). Successful exploitation of this vulnerability could enable the attacker to do a Remote Code Execution (RCE) and Local Privilege Execution (LPE), Thereby compromising the windows system.

B. Security Impact. :

An attacker can exploit this vulnerability (PrintNightmare) to take control of an affected system.

C. Affected Products and Solution:

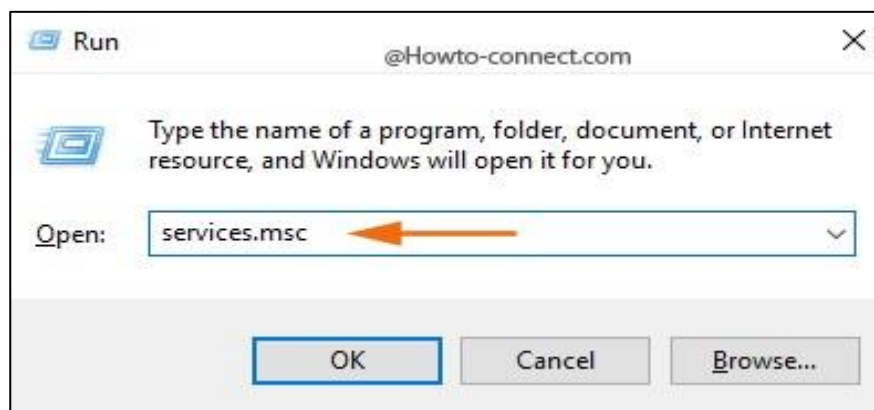
Windows Print Spooler Service. By default, this service shall be running in the background and is set to auto start at the time of windows boot.

D. Remediation:

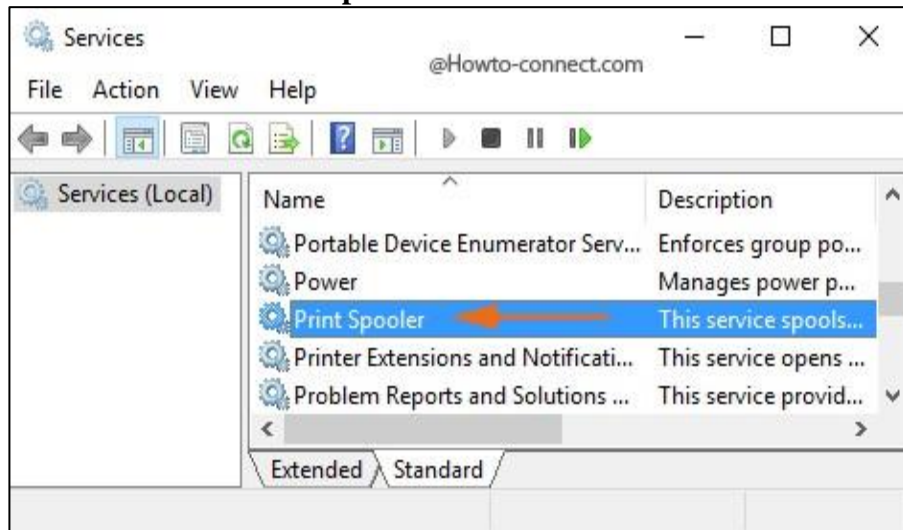
Disabling the Print Spooler service on all servers and desktops that don't require it.

Way 1 – Services

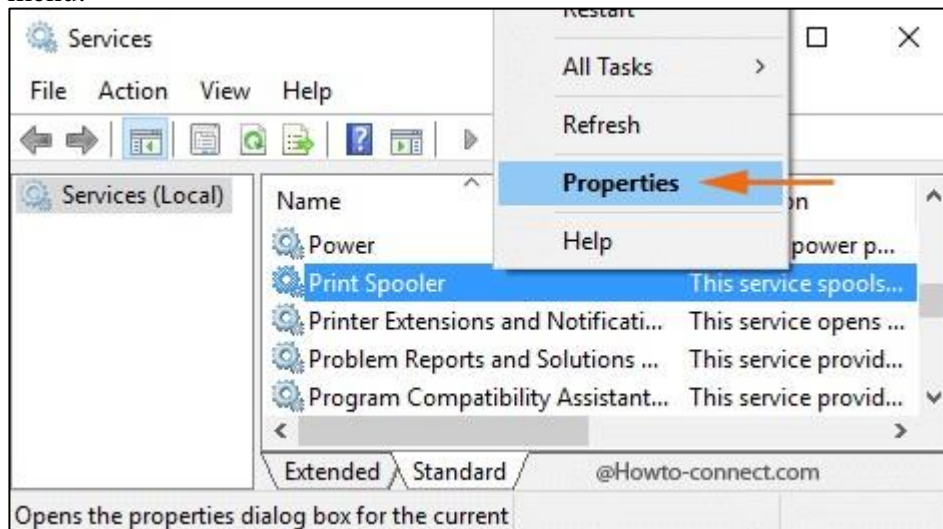
- Open Run dialog box by jointly hitting Windows +R keys and then write the code services.msc and at last hit Enter.



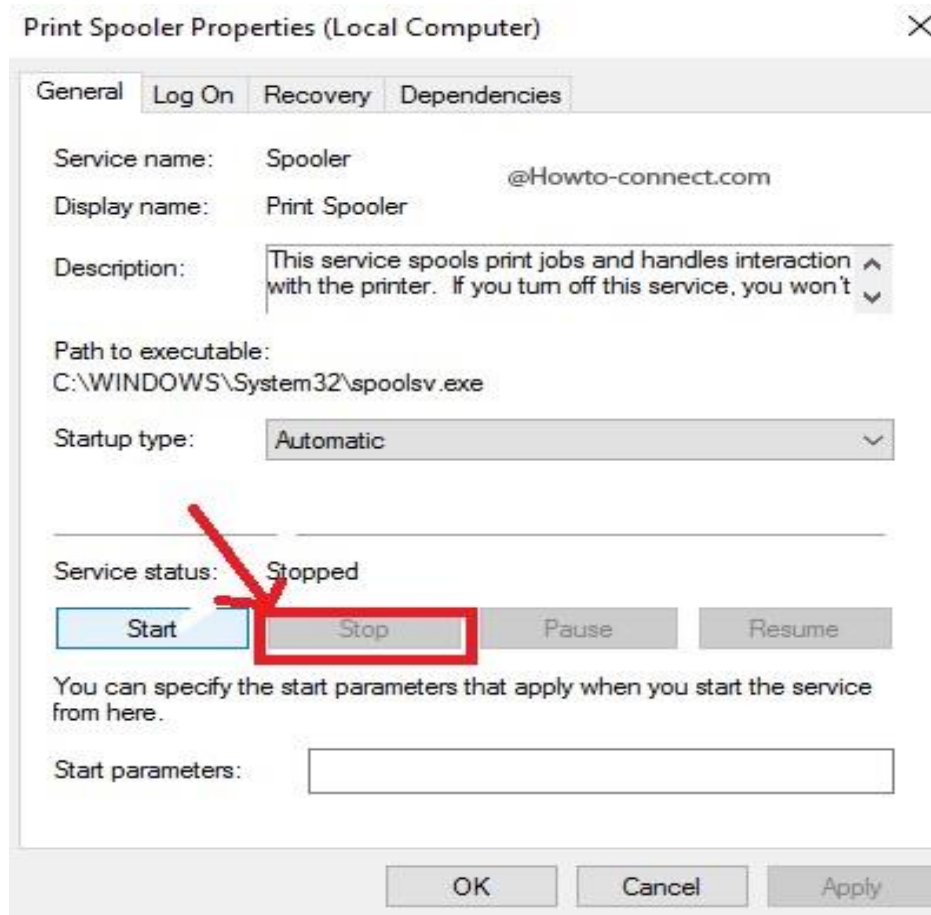
- The Services console will soon be prompted, locate the middle column and find out a service entitled as **Print Spooler**.



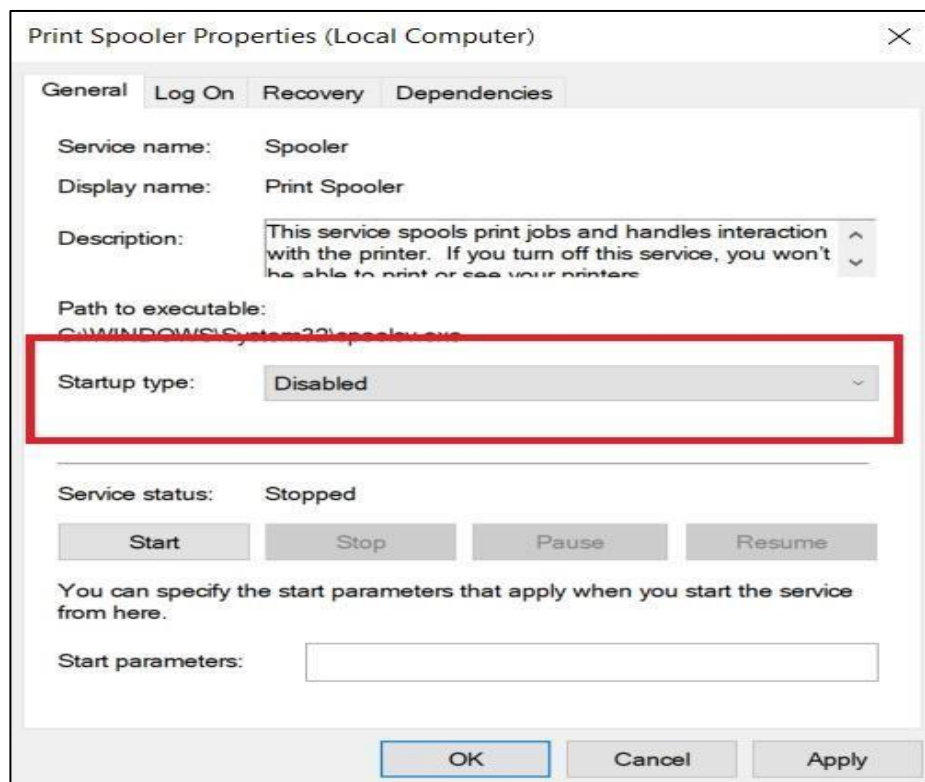
- Make a right-click on Print Spooler and tap the choice **Properties** from the emerged menu.



- Print Spooler Properties box is launched, stay into the General tab, move to the second section titled **Service status** section and hit the **Stop** button in order to Disable the service.

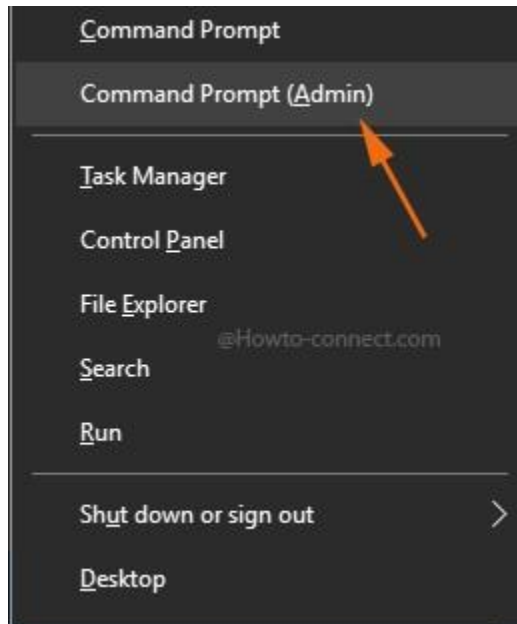


- Select Startup type: **Disabled** so that it does not start on next reboot.



Way 2 – Command Prompt

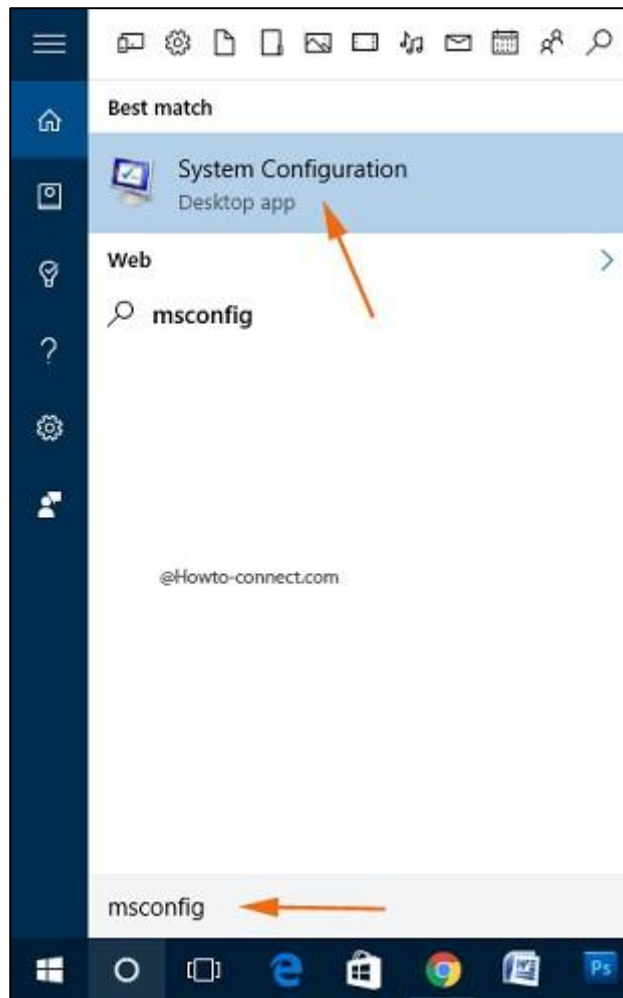
- Elevated command Prompt is compulsory to execute this tip, so jointly hit the shortcut **Windows & X** and upon the emergence of power menu, take a decision to opt the particular choice **Command Prompt (Admin)**.



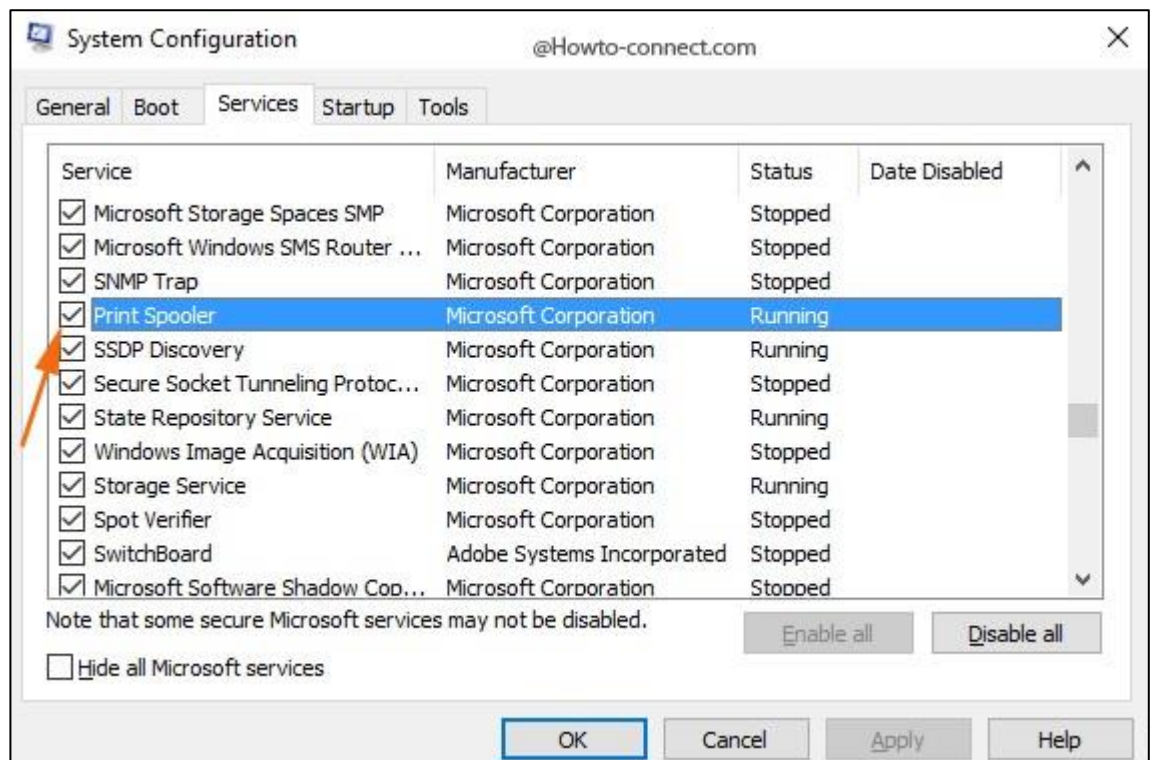
- To stop Print Spooler, copy this code `net stop spooler` and paste into the expanded elevated command prompt and finally tap on **Enter**.

Way 3 – System Configuration

- Navigate to Cortana search area, type `msconfig` in it and within no time you notice **System Configuration** just under Best match at the uppermost part, click on it.



- In the launched console, switch to the **Services** tab, the middle one and locate a service entitled as Print Spooler.
- To disable Print Spooling service, input a check mark in the square shaped tiny box and then click or hit Apply.



- **References:**

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675>