CNS IT Response to the Microsoft Spooler Service Vulnerability

Updates

Please check back here for updates M-F at 3 pm

7/22/21 12:30 pm

We will begin reaching out to users who own computers that are still having issues applying the patch.

7/20/21 3:00pm

There are no major updates today, please reboot your computer if you are still unable to print. If you can't print after a reboot and need printing sooner than later please submit a ticket to https://cns.utexas.edu/help this is still one of our highest priorities.

7/15/21 3:00pm:

There are no major updates today, please just review yesterday's notes below. If possible, please leave your computer powered on tonight as we try to get all affected computers remediated.

7/14/21 3:00pm:

There are no major updates today, please just review yesterday's notes below. If possible, please leave your computer powered on tonight as we try to get all affected computers remediated.

7/13/21 6:35pm:

For the computers that need to upgrade to newer OS first:
You will start getting popups every 4 hours to install the upgrade at 1 AM on Thursday. If you haven't installed the upgrade yet, you will get your last popup Thursday 11 pm and forced upgrade/restarts will begin Friday at 1am.

After the above upgrade and for computers with newer OS's:
We will remotely apply the hotfixes without your interaction since this one doesn't require a reboot. After the update we will lift the restriction so printing will start working, a reboot may be required.

7/13/21 2:18pm: CNS IT will begin pushing patches in short phases over the course of the week for your **Managed Windows Device(s)** to update:

- The Windows **Operating System**.
- The monthly Windows **Security Updates (July 2021)**.
- The patches released to mitigate the **Printer Spooler** service issues.

As we detect systems with **Printer Spooler** service patches applied, we'll start lifting the policies that we stopped and disabled. A reboot may be required in order to see printing available again.

7/12/21 11:07 am: We dedicated full-time support to this emergency until it is resolved. The updates released by Microsoft last week have been made available to only a subset of Windows 10 versions, and our environment is diverse with all versions of Windows 10. For older versions of 10 to work, computers need to be upgraded, so we have been working on a solution to enable end-users to do this as multiple restarts are required, and we do not want to disrupt end-users further. When a patch is released, we do due diligence by testing the update on diverse environments before sending it out to computers to potentially catch any issues (especially in a patch that was released in an emergency). We are working through computers that do not require the upgrade first, then will move to the older versions of Windows 10. If you need printing sooner, please submit a ticket to **help@cns.utexas.edu**, and we will help remediate it. More updates to come at 3 pm.

What is this about?

CNS IT will be setting a policy to disable the Print Spooler Service on managed Windows systems on Thursday, July 1, 2021 at 7:00am CST.

Why is this happening?
A critical exploit has been identified in most Windows systems, involving the Print Spooler Service. At this time, a fix hasn't been released. Until a fix exists, the UT Information Security Team has requested that the Print Spooler Service be disabled on Windows systems at UT Austin. More information on the vulnerability can be found here: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

What will happen if my computer isn't made compliant?
The ISO will be quarantining devices as soon as they can scan for this vulnerability. We have a short grace period until that happens to get the Spooler Service disabled and turned off.

How to upgrade/update your computer:

Follow these instructions for BOTH Managed Software Updates then "All other PC's". Note depending on the network you are on just following the Managed Software Updates instructions will not work.

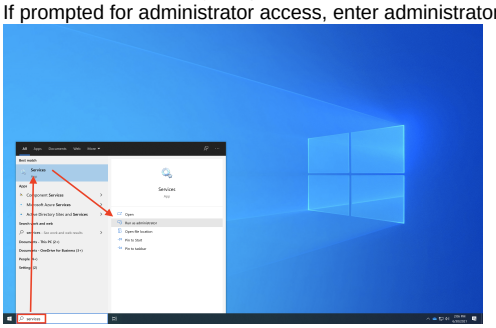
Computers installed and configured by CNS IT:

We will be disabling the Spooler Service as a policy that will automatically adjust the Print Spooler Service on your computer. Please run through the following to make sure that the policy has successfully disabled your Print Spooler Service.

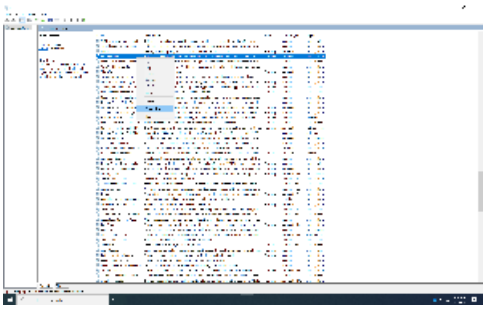
Computers that weren't set up and configured by CNS IT:

Since CNS IT doesn't remotely manage your computer, here are some steps you can follow to manually disable the Print Spooler Service on your Windows device.

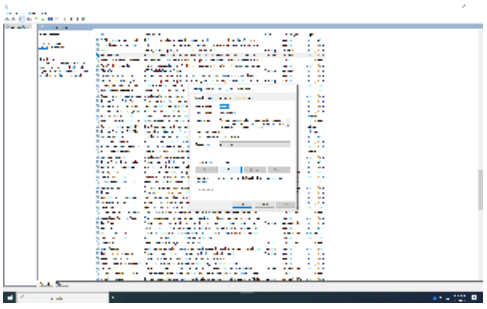
1. Open the Services snap-in.
    a. You can find it by searching for 'Services' in the bar next to the Start menu (Windows 10) or at the bottom of the start menu (Windows 7).
    b. Run the Services snap-in as administrator, on the right side of the Start screen (Windows 10) or by right-clicking (Windows 7 and some custom Windows 10 layouts).
    c. If prompted for administrator access, enter administrator account credentials if you have them.



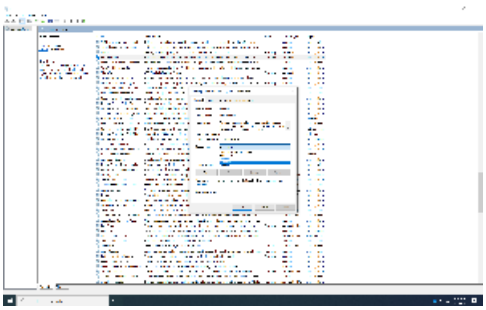
2. Find the Print Spooler Service, right-click it, select to `Properties`.



3. Press `Stop` in the Properties window to stop the Spooler Service.



4. Set the startup type to `disabled` to make sure the Service won't start again when you reboot.



5. Make sure you Press Apply and OK before you close the Services window.