UBND TỈNH THANH HOÁ
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Số: 7772 /STNMT-DLTT

V/v cảnh báo các lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 08/2024.

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Thanh Hoá, ngày 26 tháng 8 năm 2024

Kính gửi: Trưởng các đơn vị thuộc Sở

Sở Tài nguyên và Môi trường nhận được Công văn số 273/TTCNTT&TT-QTHT ngày 22/8/2024 của Trung tâm Công nghệ thông tin và Truyền thông về việc cảnh báo các lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 08/2024. Trên cơ sở cung cấp thông tin về danh sách bản vá tháng 08 với 90 lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft ngày 13/8/2024 tại Công văn số 1667/CATTT-NCSC ngày 19/08/2024 về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 08/2024 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Cụ thể như sau:

(1) Lỗ hổng an toàn thông tin CVE-2024-38063 trong Windows TCP/IP cho phép đối tượng tấn công thực thi mã từ xa..

(2) Lỗ hổng an toàn thông tin CVE-2024-38199 trong Windows Line Printer Daemon (LPD) Service cho phép đối tượng tấn công thực thi mã từ xa. Thông tin chi tiết về lỗ hổng đã được công bố công khai.

(3) Lỗ hổng an toàn thông tin CVE-2024-38189 trong Microsoft Project cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế.

(4) 02 lỗ hổng an toàn thông tin CVE-2024-38218, CVE-2024-38219 trong Microsoft Edge cho phép đối tượng tấn công thực thi mã từ xa.

(5) Lỗ hổng an toàn thông tin CVE-2024-38193 trong Windows Ancillary Function Driver for WinSock cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

(6) Lỗ hổng an toàn thông tin CVE-2024-38107 trong Windows Power Dependency Coordinator cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

Ngoài các lỗ hổng an toàn thông tin nêu trên, còn tồn tại một số lỗ hổng an toàn thông tin khác có thể ảnh hưởng đến hệ thống thông tin của các đơn vị

(Thông tin chi tiết các lỗ hổng bảo mật có tại Phụ lục kèm theo)

Để tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại các

hệ thống thông tin và máy tính của các đơn vị, Giám đốc Sở có ý kiến chỉ đạo như sau:

1. Giao Trưởng các đơn vị trực thuộc Sở chỉ đạo các bộ phận, cá nhân thực hiện:

- Chủ động kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng *(nếu có)*. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công.

- Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc liên hệ với Tổ ứng cứu sự cố An toàn thông tin mạng Sở Tài nguyên và Môi trường hoặc Trung tâm Dữ liệu thông tin tài nguyên và môi trường (đơn vị phụ trách an toàn thông tin mạng của Sở trực tiếp theo dõi, chỉ đạo hoạt động của Tổ ứng cứu sự cố).

2. Giao Trung tâm Dữ liệu thông tin tài nguyên và môi trường:

- Tổ chức kiểm tra, rà soát và xác định máy tính trong phạm vi cơ quan đang sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng (nếu có), thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công.

- Chỉ đạo Tổ ứng cứu sự cố Sở, tổ chức tiến hành kiểm tra, rà soát và khoanh vùng tìm kiếm để gỡ bỏ mã độc đang lây nhiễm trên các máy tính trong hệ thống mạng của Sở, xử lý, ngăn chặn sự cố mất an toàn thông tin nếu có tại Cơ quan Sở và các đơn vị trực thuộc Sở Tài nguyên và Môi trường.

- Đăng tải hướng dẫn kỹ thuật cách thức thực hiện chi tiết đối với lỗ hổng bảo mật lên Cổng thông tin điện tử của Sở.

Theo các nội dung trên, yêu cầu các đơn vị nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Giám đốc Sở (để b/c);
- Các đồng chí Trưởng đơn vị (để thực hiện);
- Cổng thông tin điện tử Sở;
- Lưu: VT, TTDLTTTNMT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TỈNH THANH HÓA

Nguyễn Khánh Toàn

Phụ lục:

THÔNG TIN CÁC LỖ HỔNG BẢO MẬT THÁNG 8/2024

1. Thông tin các lỗ hổng bảo mật:

STT	CVE	Mô tả	Linh tham khảo
1	CVE-2024-38063	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows TCP/IP cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063
2	CVE-2024-38199	- Điểm CVSS: 9.8 (Cao) - Mô tả: Lỗ hổng trong Windows Line Printer Daemon (LPD) Service cho phép đối tượng tấn công thực thi mã từ xa. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199
3	CVE-2024-38189	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Project cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Project 2016, Microsoft Office 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189
4	CVE-2024-38218 CVE-2024-38219	- Điểm CVSS: 8.4 (Cao) - Mô tả: Lỗ hổng trong Microsoft Edge cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Edge (Chromium-based).	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38218 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38219

5	CVE-2024-38193	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Ancillary Function Driver for WinSock cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193
6	CVE-2024-38107	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Power Dependency Coordinator cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107
7	CVE-2024-38170 CVE-2024-38172	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft 365 Apps for Enterprise, Microsoft Office LTSC for Mac 2021..	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38170 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38172
8	CVE-2024-38171	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft PowerPoint cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft PowerPoint 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38171
9	CVE-2024-38178	- Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng trong Scripting Engine cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178

		hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.	
10	CVE-2024-38202	- Điểm CVSS: 7.3 (Cao) - Mô tả: Lỗ hổng trong Windows Update Stack cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38202
11	CVE-2024-38106	- Điểm CVSS: 7.0 (Cao) - Mô tả: Lỗ hổng trong Windows Kernel cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106
12	CVE-2024-21302	- Điểm CVSS: 6.7 (Cao) - Mô tả: Lỗ hổng trong Windows Secure Kernel Mode cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302
13	CVE-2024-38173	- Điểm CVSS: 6.7 (Cao) - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Outlook 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38173

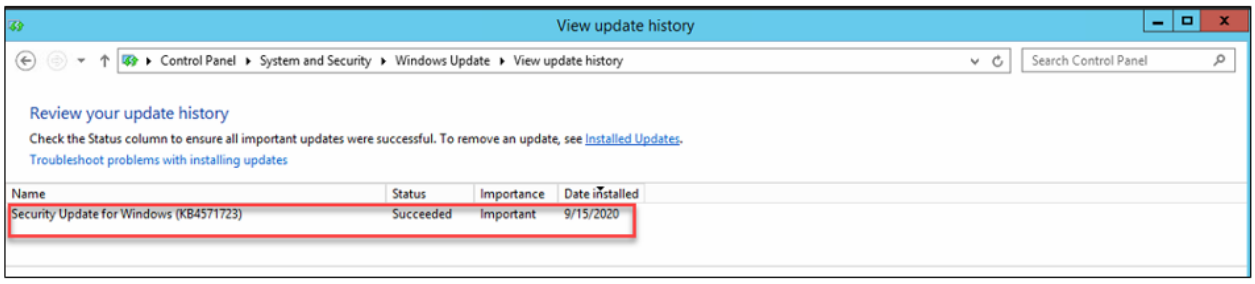
14	CVE-2024-38200	- Điểm CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Microsoft Office 2016, 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200
15	CVE-2024-38213	- Điểm CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Windows Mark of the Web Security cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213

2. Hướng dẫn khắc phục:

Phương pháp 1: Kiểm tra lịch sử cập nhật trên máy chủ

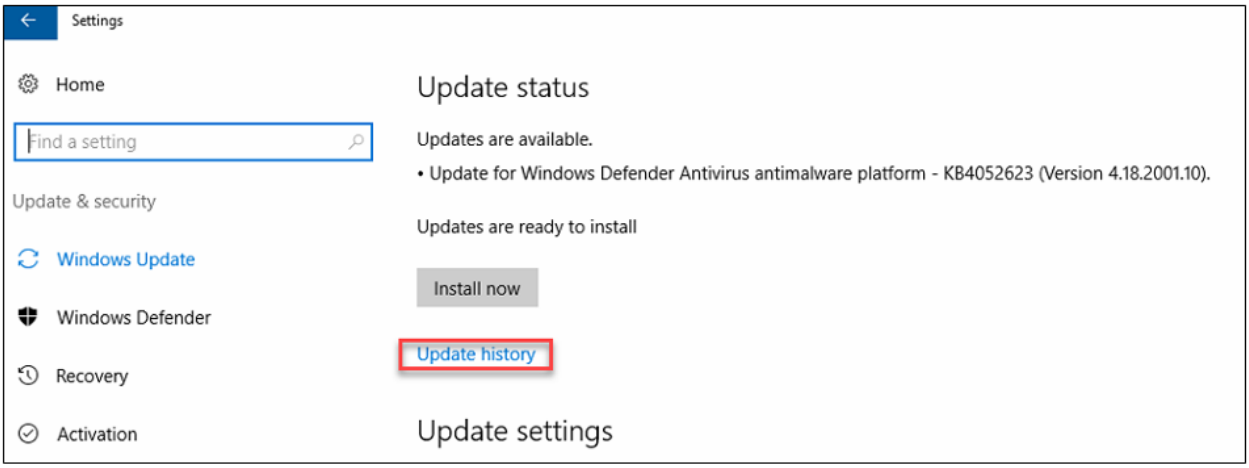
- Windows Server 2012:

Truy cập **Windows Update** > **View update history** > Kiểm tra mã bản cập nhật đã đúng với mã phiên bản cần cập nhật tại mục **2.1.**



- Windows Server 2016 trở lên/ Windows 10:

Truy cập **Setting** > **Update & Security** > **Update history** > Kiểm tra mã bản cập nhật đã đúng với mã phiên bản cần cập nhật tại mục **2.1.**



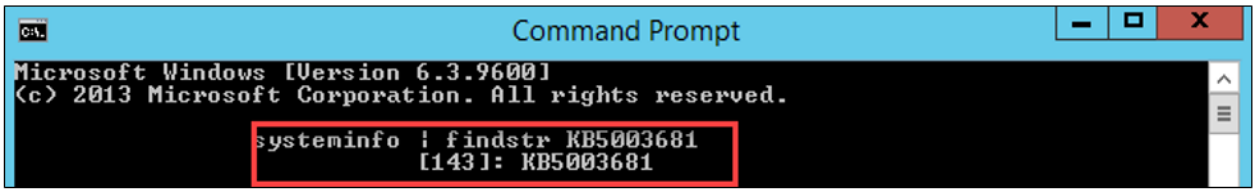
Phương pháp 2: Sử dụng CommandLine

- Cách thức truy cập CommandLine:

+ Vào thanh công cụ **Start** > **Run** > gõ **cmd.exe** và chọn **OK**
+ Vào thanh công cụ **Start** > Gõ **cmd** tại ô tìm kiếm và ấn **ENTER**
Sử dụng lệnh **systeminfo** | **findstr KB**(mã **kb** tại mục **2.1**)

- Ví dụ: systeminfo | findstr KB5003681

+ Với những máy chủ đã update sẽ hiện thông tin:

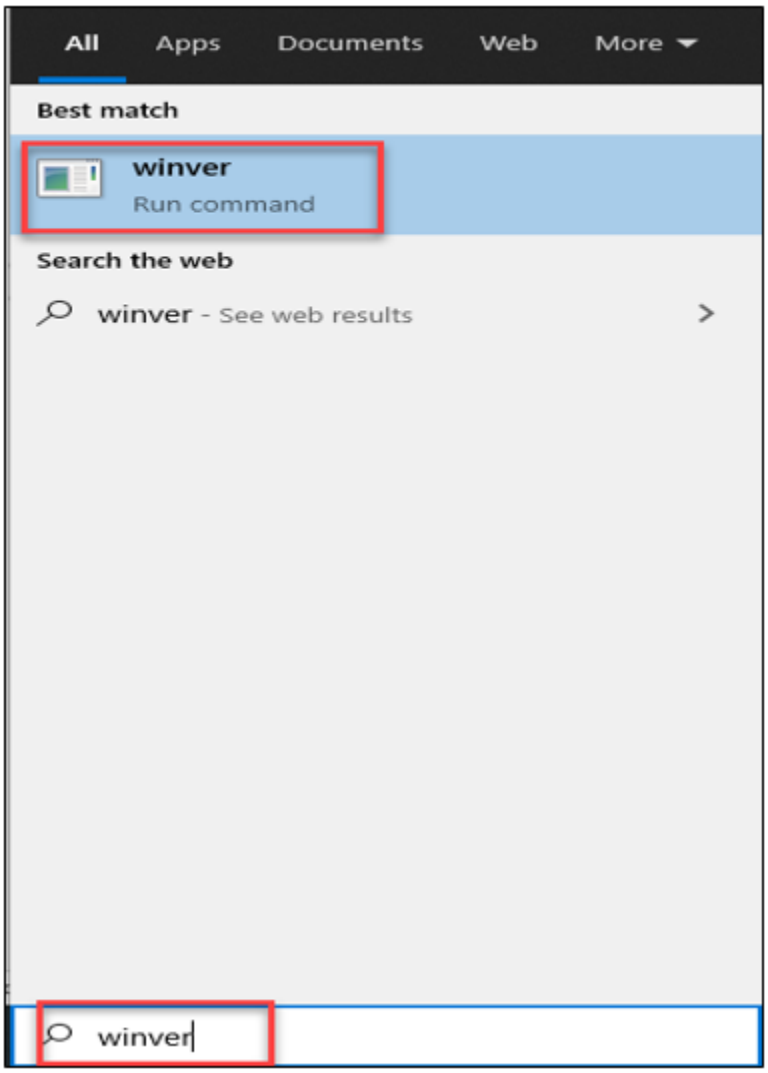


+ Với những máy chủ chưa update, sẽ không hiện ra thông tin:

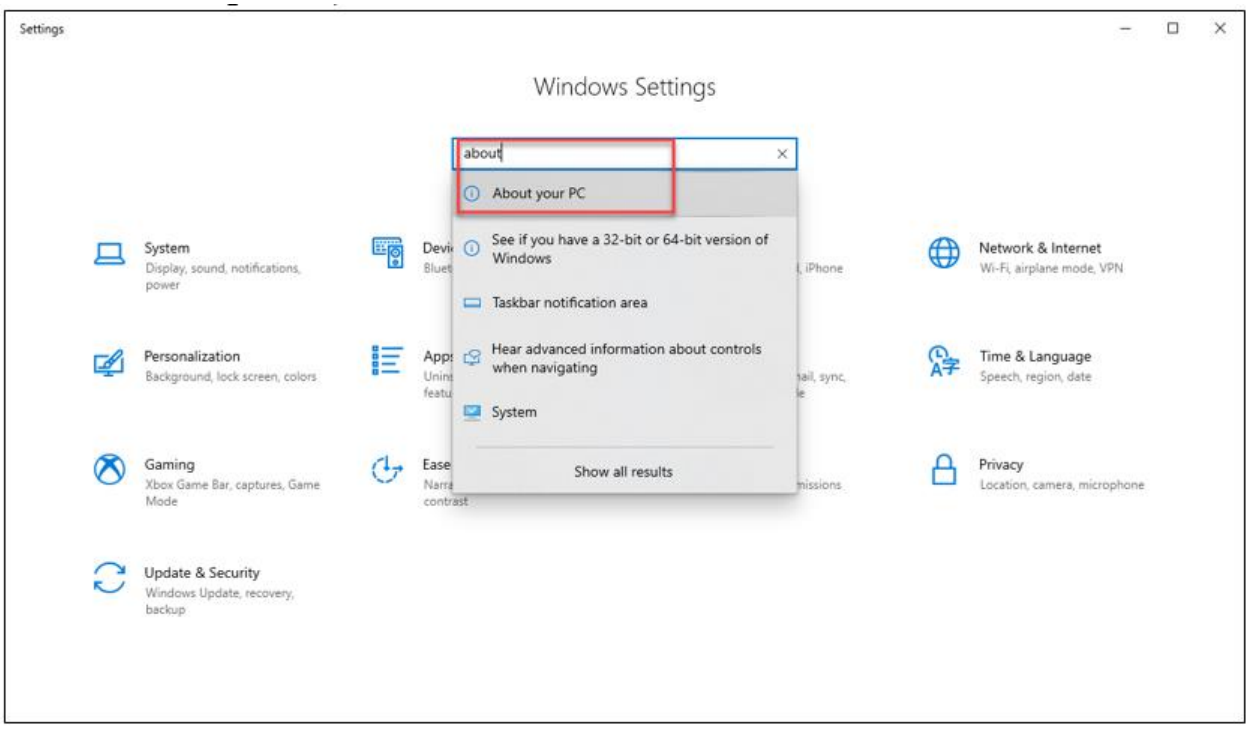
3. Hướng dẫn thực hiện cập nhật bản vá
3.1. Đối với hệ thống không có máy chủ WSUS

- Bước 1: Kiểm tra OS, version hệ điều hành đang sử dụng:

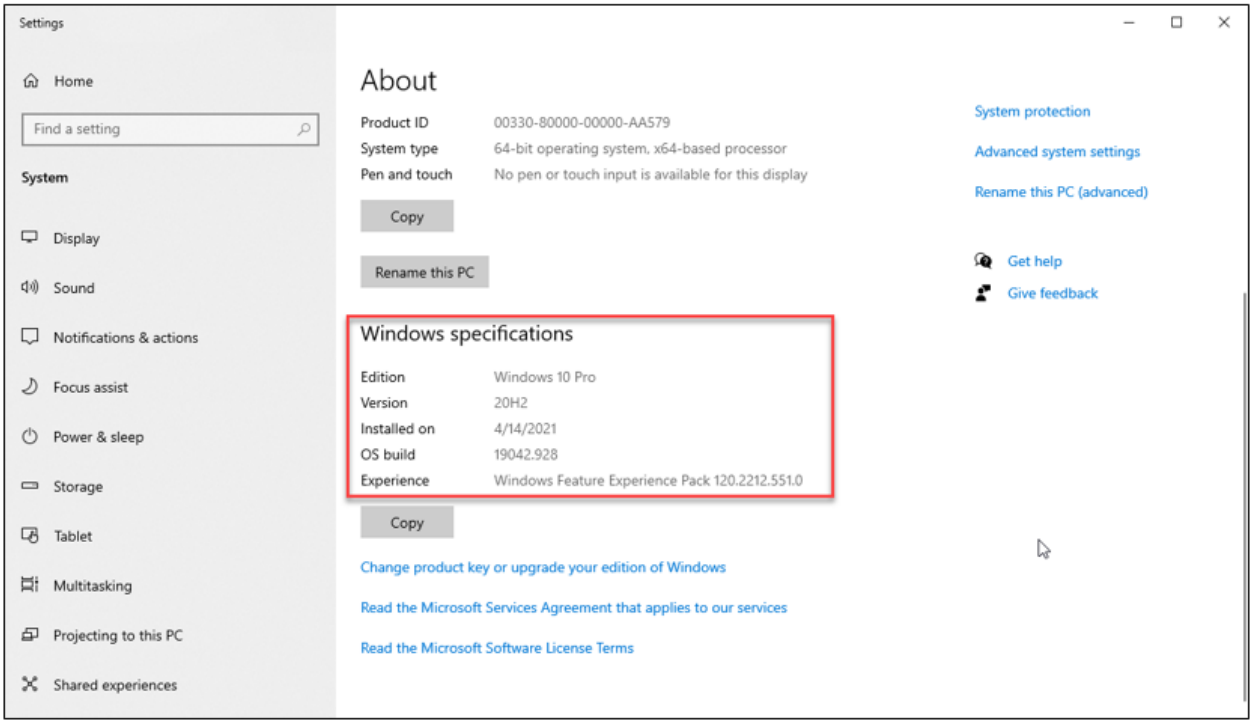
Cách 1: Chọn thanh **Start** > Gõ **winver** > **Enter** để kiểm tra:



Cách 2: Chọn **Setting** > Nhập ô tìm kiếm "**About this PC**" (hoặc chuột phải **This PC** > **Properties**)



Kiểm tra mục: **Windows Specifications**

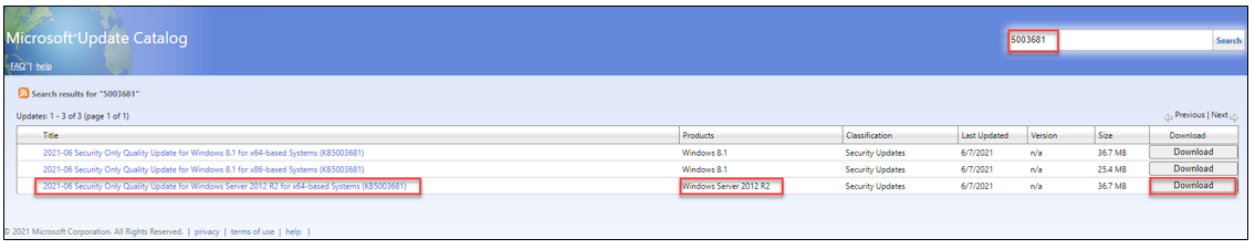


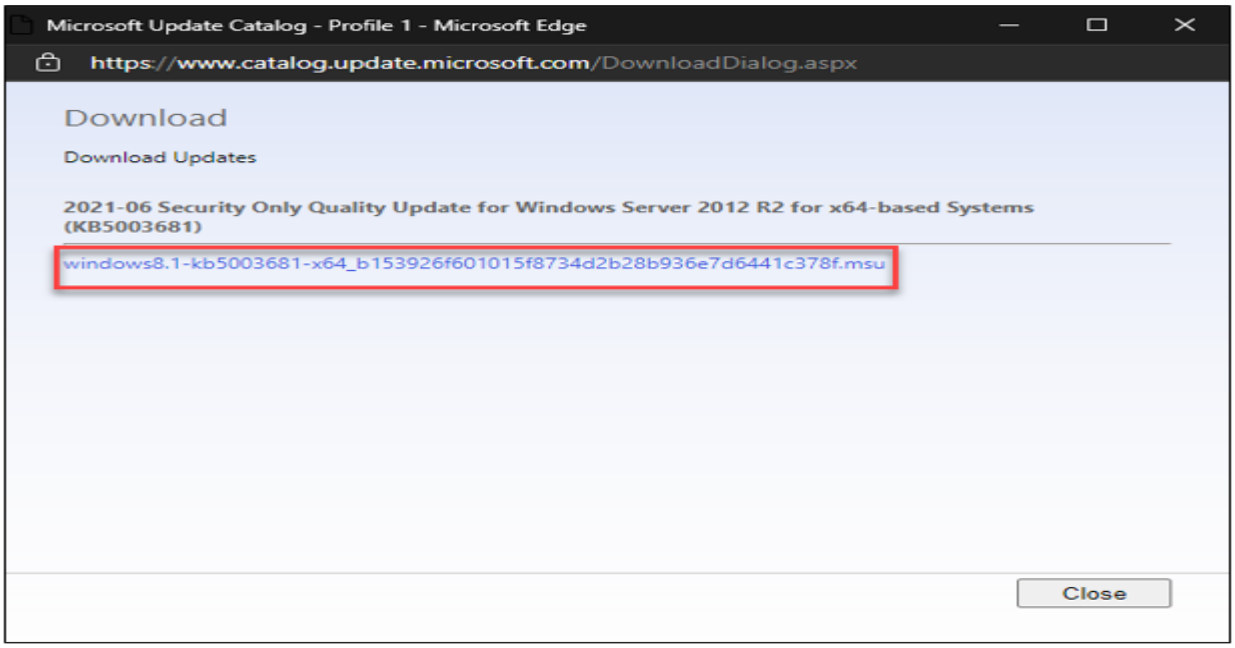
- Bước 2: Download bản vá tại

https://www.catalog.update.microsoft.com/Home.aspx

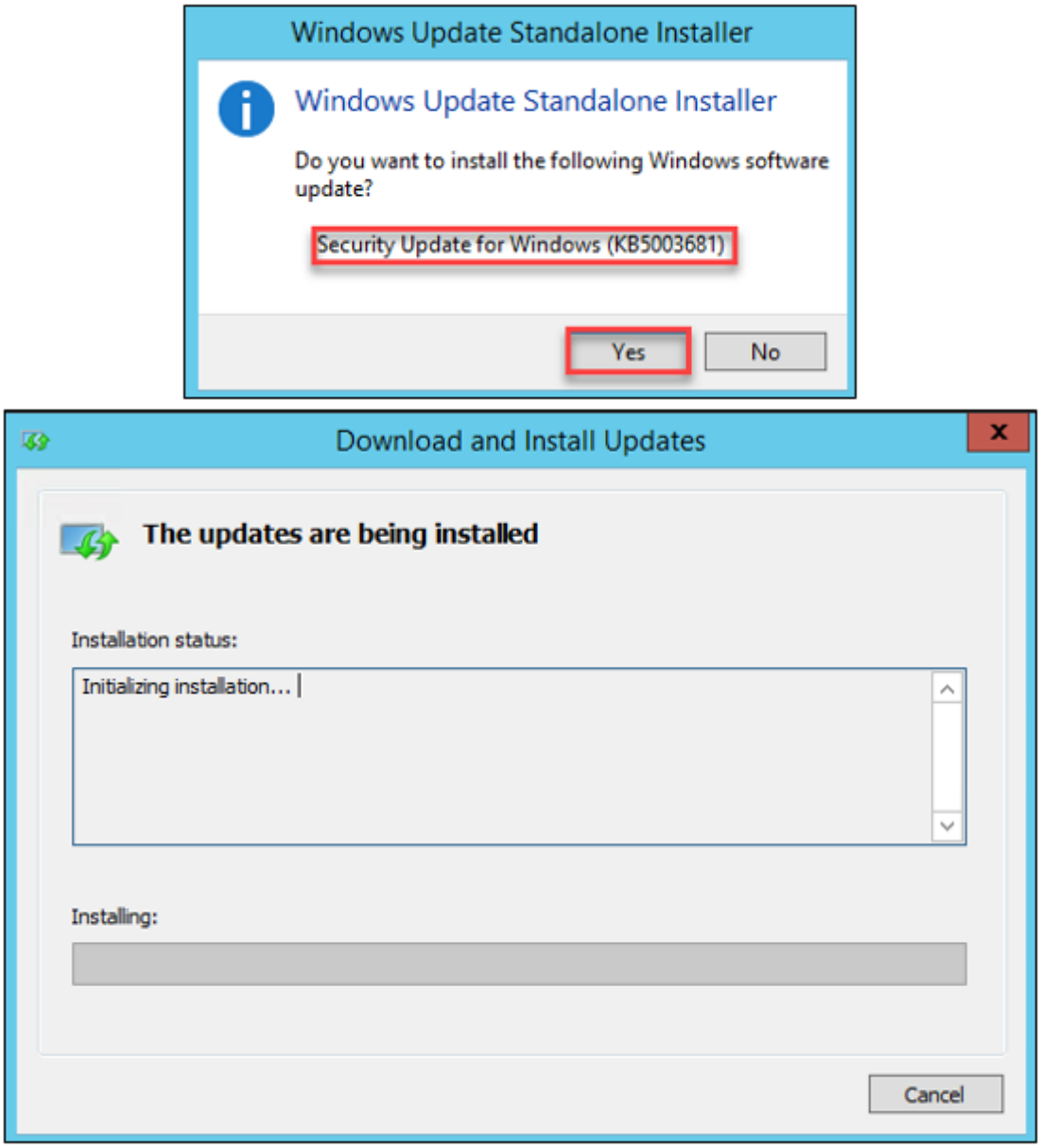
Tại ô **Search** nhập mã **kb** phù hợp dựa vào bảng trên mục **2.1**

- Bước 3: Tìm và tải bản cập nhật phù hợp cho máy chủ hệ điều hành





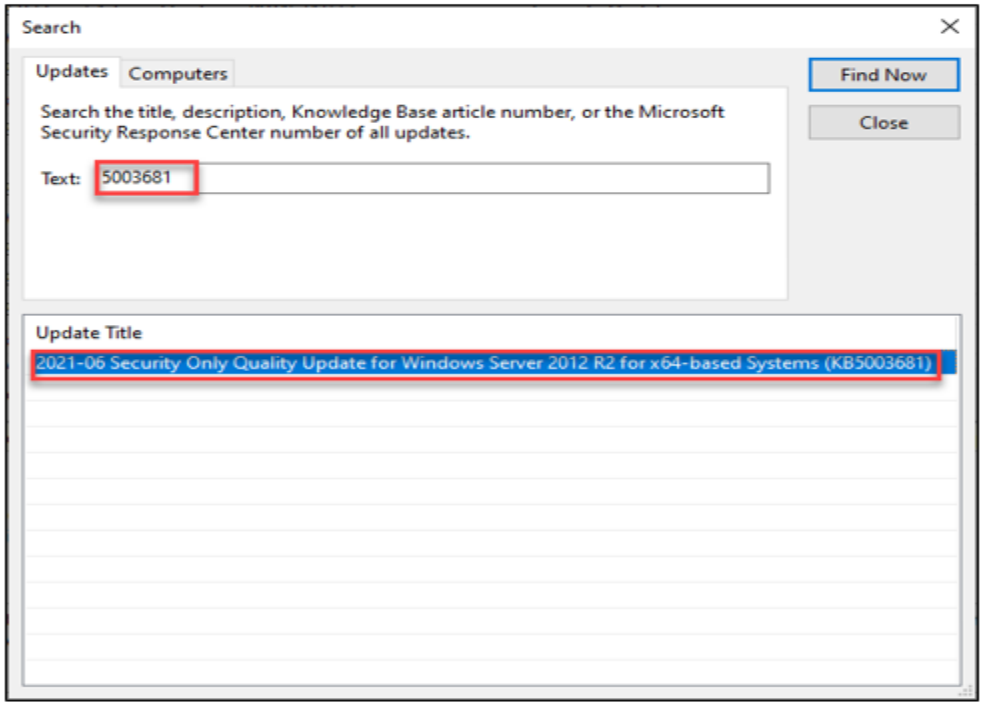
- Bước 4: Cài đặt bản cập nhật đã tải lên từng máy



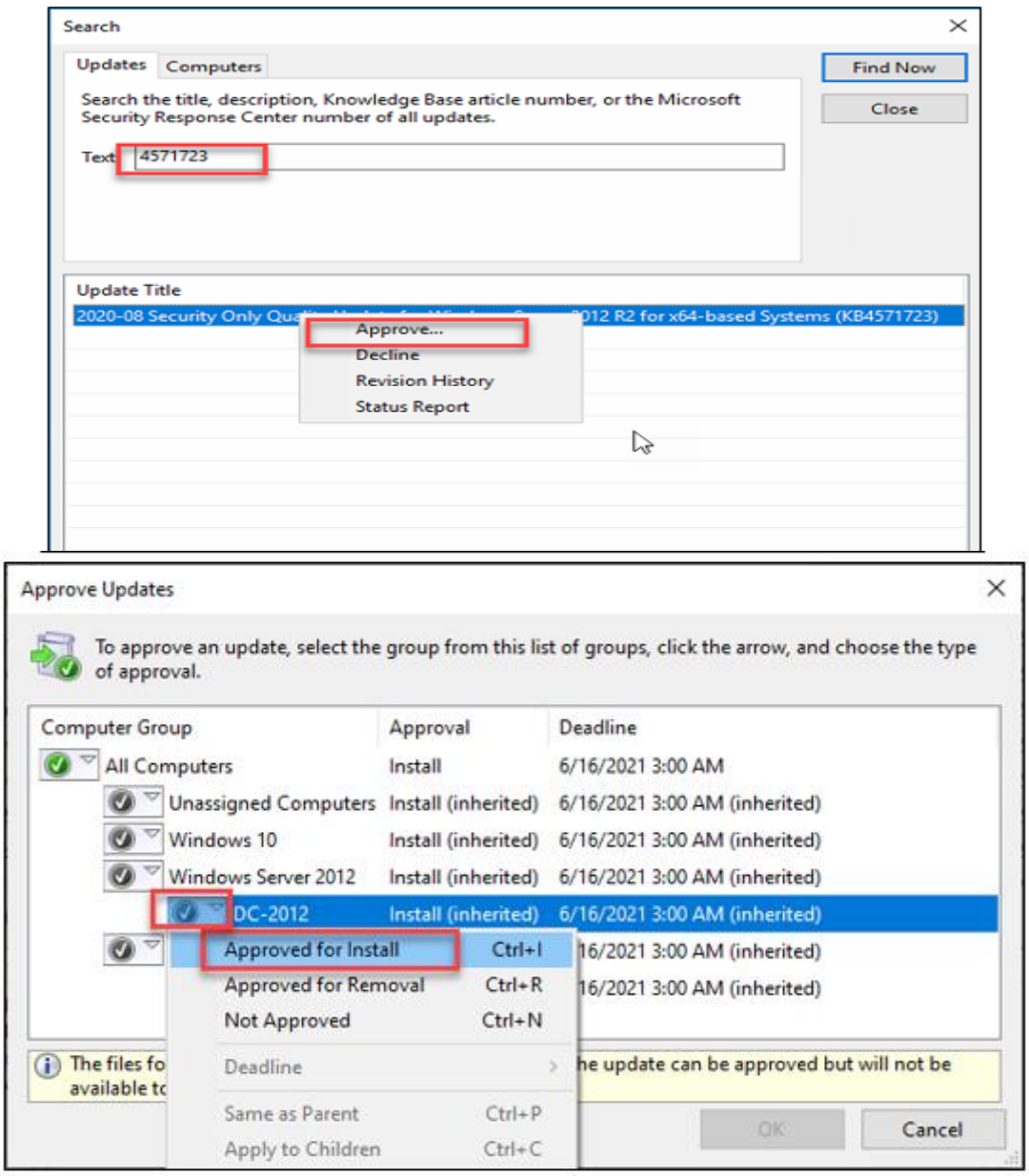
- Bước 5: Khởi động lại máy chủ sau khi tiến hành cài đặt bản cập nhật.

3.2. Đối với hệ thống sử dụng WSUS

- Bước 1: Với các hệ thống sử dụng máy chủ WSUS để quản trị các bản cập nhật tập trung, nhập mã **kb** phù hợp dựa vào bảng trên mục **2.1.**



- Bước 2: Chọn **Approve** và chọn group hệ điều hành phù hợp với bản update



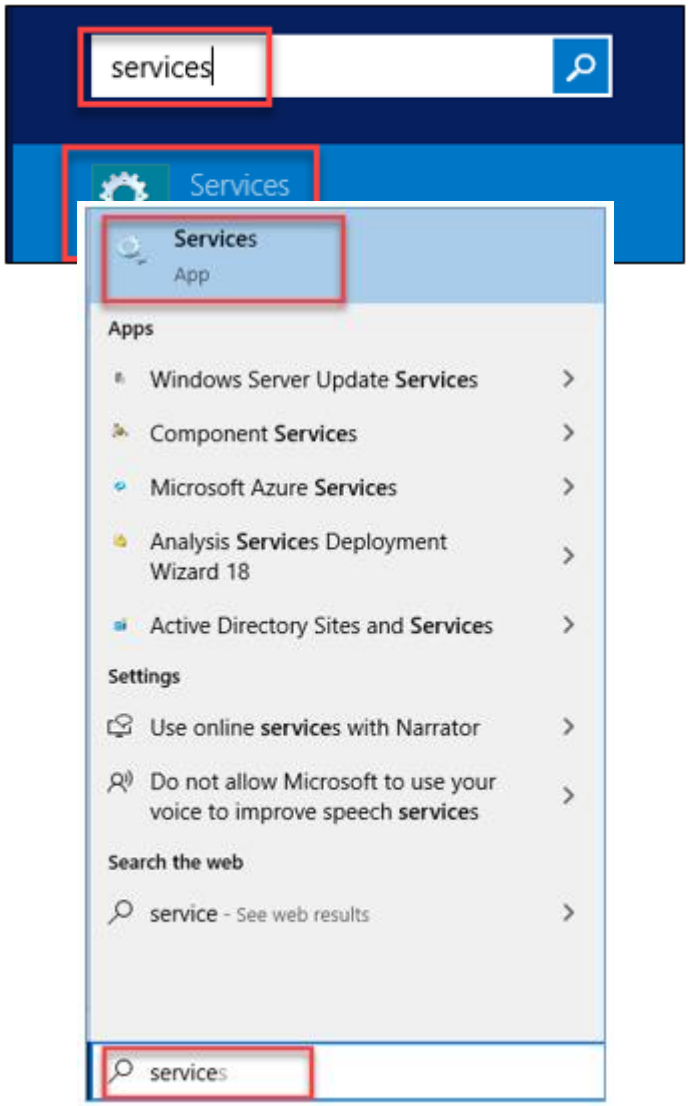
- Bước 3: Cài đặt bản cập nhật và khởi động lại máy chủ.

3.3. Kiểm tra lại bản cài đặt trên máy chủ

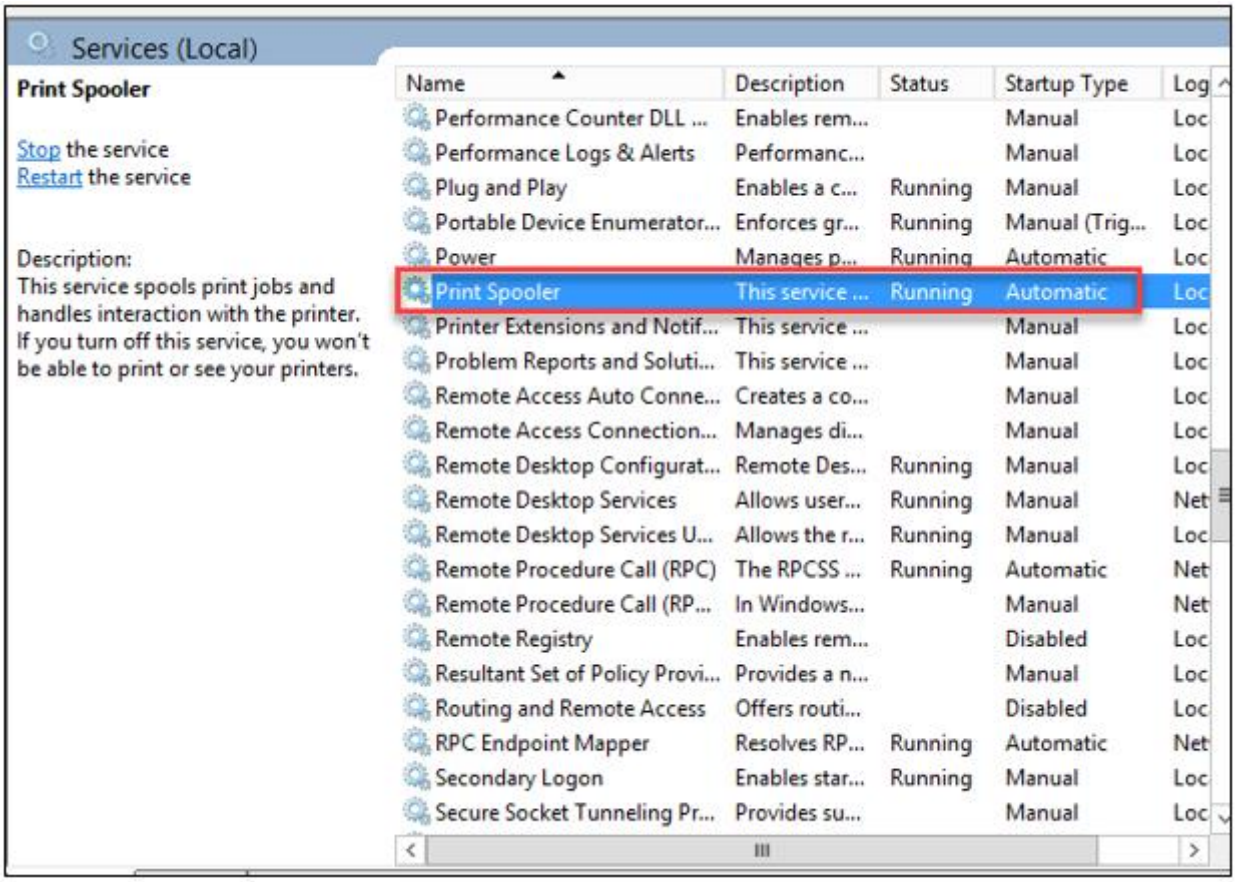
Các bước thực hiện tương tự ở mục **2.2.**

4. Đối với những hệ thống chưa cập nhật được DC

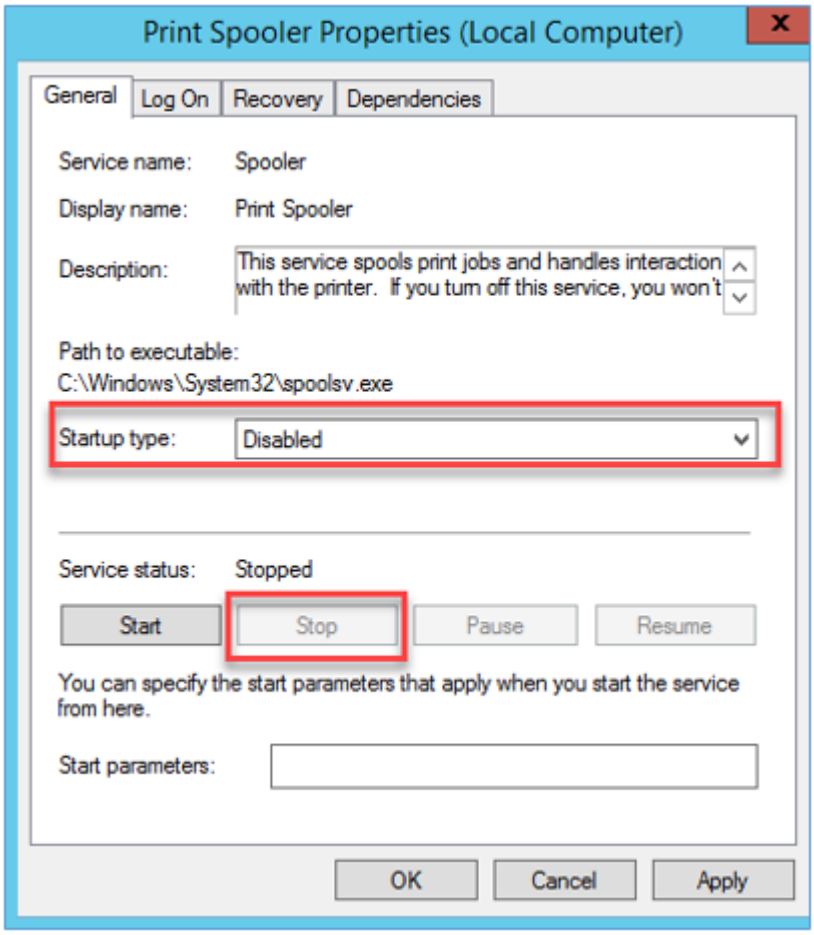
- Bước 1: Vào máy chủ DC, chọn **Start** > Nhập **services.msc** > **Enter**



- Bước 2: Tại mục **Services**, tìm đến mục **Print Spooler** > chuột phải chọn **Properties**



- Bước 3: Chọn **Startup Type: Disable; Services Status: Stop**



- Bước 4: Chọn **OK** để hoàn thành thiết lập.

3. Tà i liệ u tham khả o

https://msrc.microsoft.com/update-guide/

https://www.zerodayinitiative.com/blog/2024/8/13/the-august-2024-security-update-review