UBND TỈNH THANH HOÁ
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Số: 2828 /STNMT-DLTTTNMT

V/v cảnh báo và phòng ngừa các lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2024.

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

Thanh Hoá, ngày 03 tháng 4 năm 2024

Kính gửi: Trưởng các đơn vị thuộc Sở

Sở Tài nguyên và Môi trường nhận được Công văn số 111/TTCNTT&TT-QTHT ngày 28/3/2024 của Trung tâm Công nghệ thông tin và Truyền thông về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2024. Theo đó, ngày 12/3/2024, Microsoft đã phát hành danh sách bản vá tháng 3 với 59 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

(1) Lỗ hổng an toàn thông tin CVE-2024-26198 trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

(2) Lỗ hổng an toàn thông tin CVE-2024-21407 trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.

(3) Lỗ hổng an toàn thông tin CVE-2024-21408 trong Windows Hyper-V cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS).

(4) Lỗ hổng an toàn thông tin CVE-2024-21334 trong Open Management Infrastructure (OMI) cho phép đối tượng tấn công thực thi mã từ xa.

(5) Lỗ hổng an toàn thông tin CVE-2024-21426 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

(6) Lỗ hổng an toàn thông tin CVE-2024-21411 trong Skype for Consumer cho phép đối tượng tấn công thực thi mã từ xa.

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. 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 Công nghệ thông tin (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.

- Tham mưu công văn gửi Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa *(cơ quan thường trực của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh)* trước ngày 10/4/2024 về kết quả thực hiện.

- 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 t/h);
- 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

(Kèm theo công văn số /STNMT-DLTTTNMT ngày tháng năm 2024 của Sở Tài nguyên và Môi trường)

1. Thông tin các lỗ hổng bảo mật:

STT	CVE	Mô tả	Linh tham khảo
1	CVE-2024-26198	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE2024-26198
2	CVE-2024-21407	- Điểm: CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2012, 2012 R2, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE2024-21407
3	CVE-2024-21408	- Điểm: CVSS: 5.5 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS). - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE2024-21408
4	CVE-2024-21334	- Điểm: CVSS: 9.8 (Cao) - Mô tả: Lỗ hổng trong Open Management Infrastructure (OMI) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: OMI; System Center Operations Manager (SCOM) 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE2024-21334
5	CVE-2024-21426	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Enterprise Server 2016, Microsoft	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21426

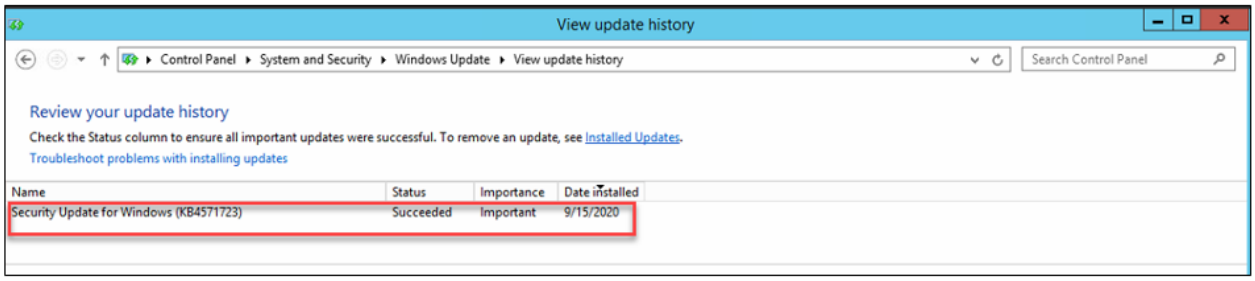
		SharePoint Server 2019; Microsoft SharePoint Server Subscription Edition.	
6	CVE-2024-21411	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Skype for Consumer cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Skype for Consumer.	https://msrc.microsoft.com/update-guide/vulnerability/CVE2024-21411

2. Hướng dẫn khắc phục:

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

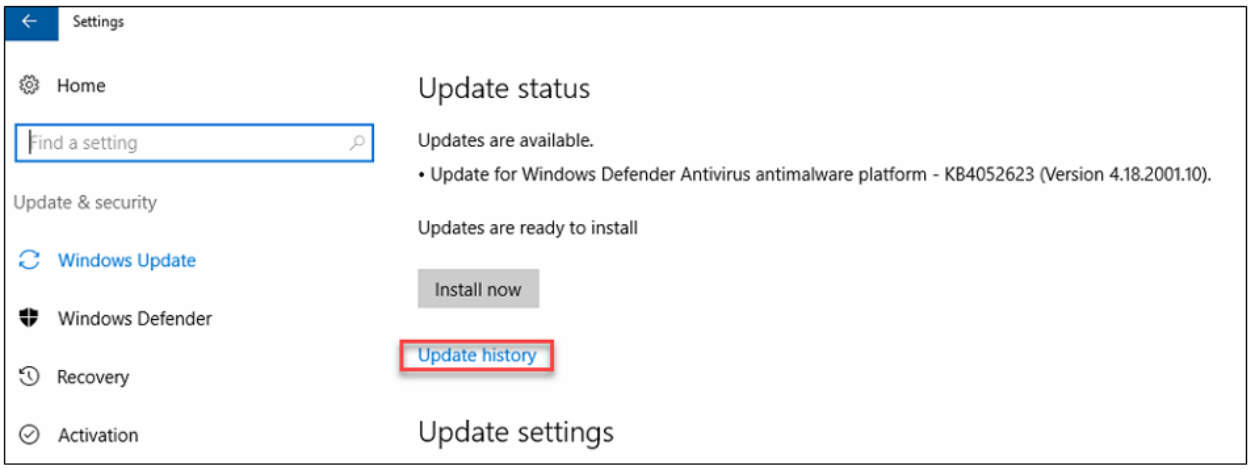
- Windows Server 2012:

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.**



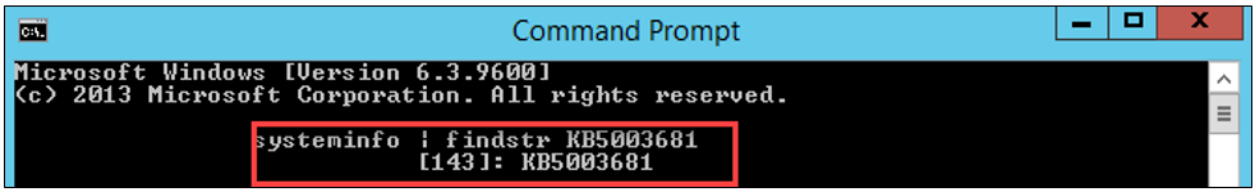
Phương pháp 2: Sử dụng CommandLine

- 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:

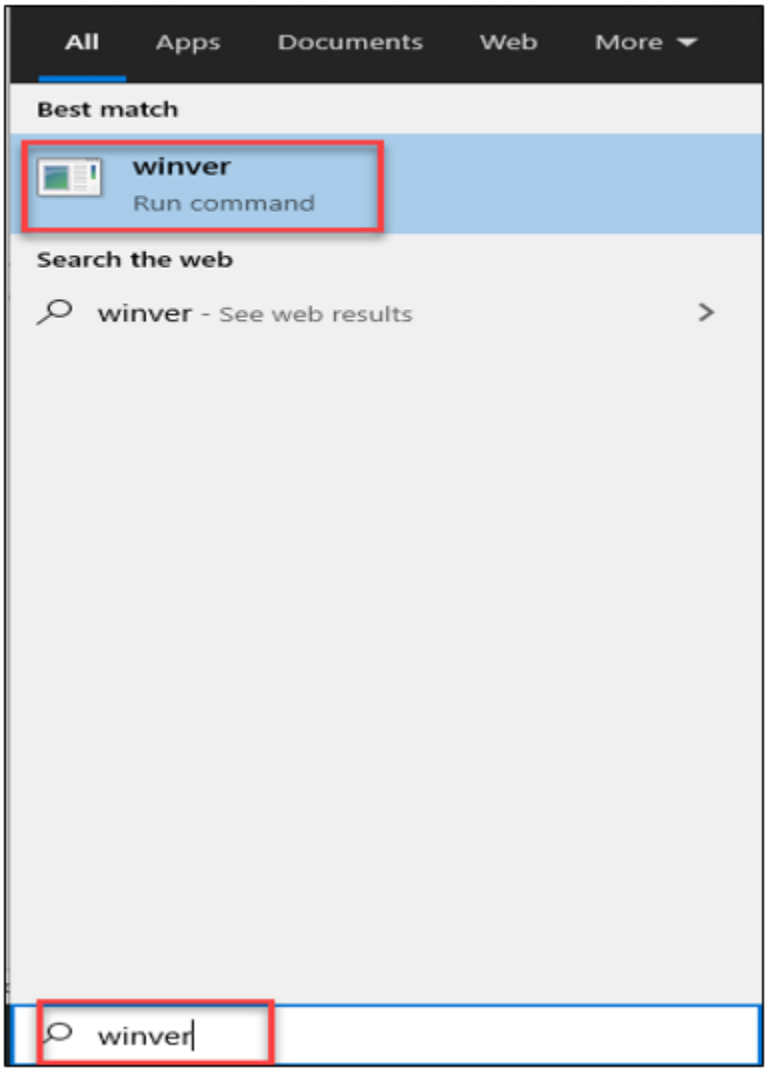


+ Với những máy chủ chưa update, sẽ không hiện ra thông tin:

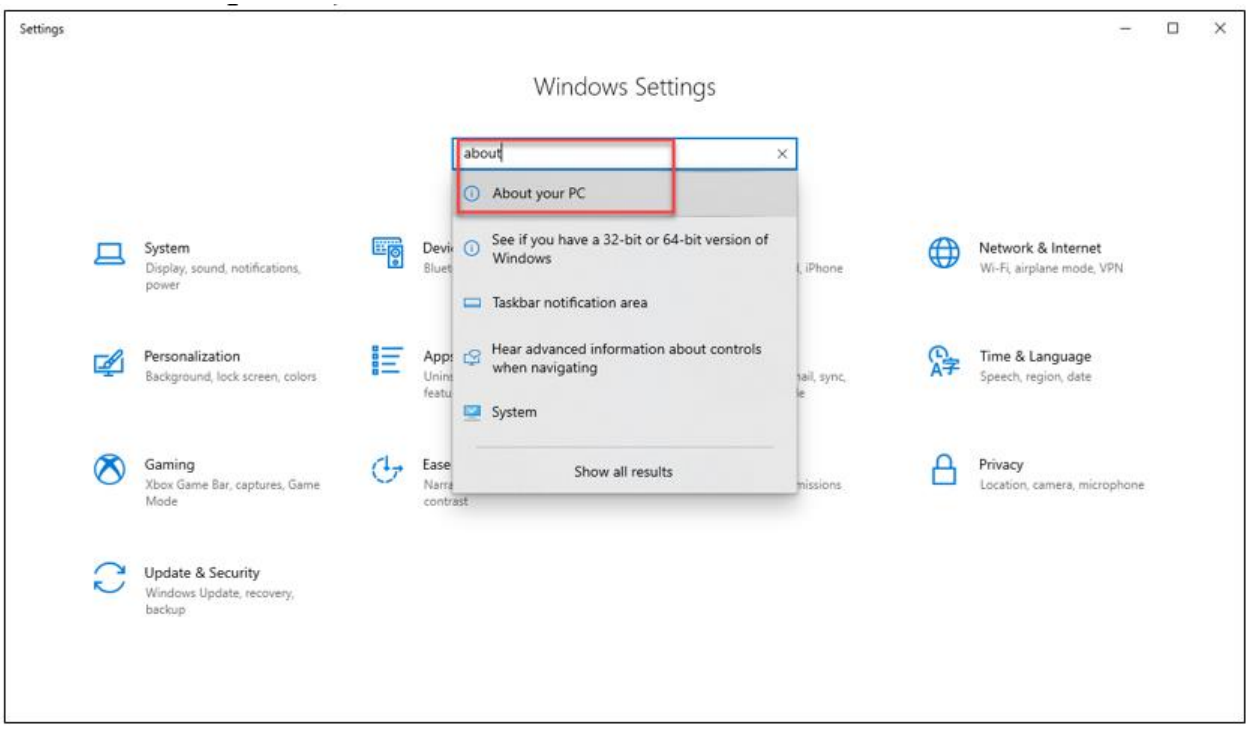
3. Hướng dẫn thực hiện cập nhật bản vá
3.1. Đối với hệ thống không có máy chủ WSUS

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

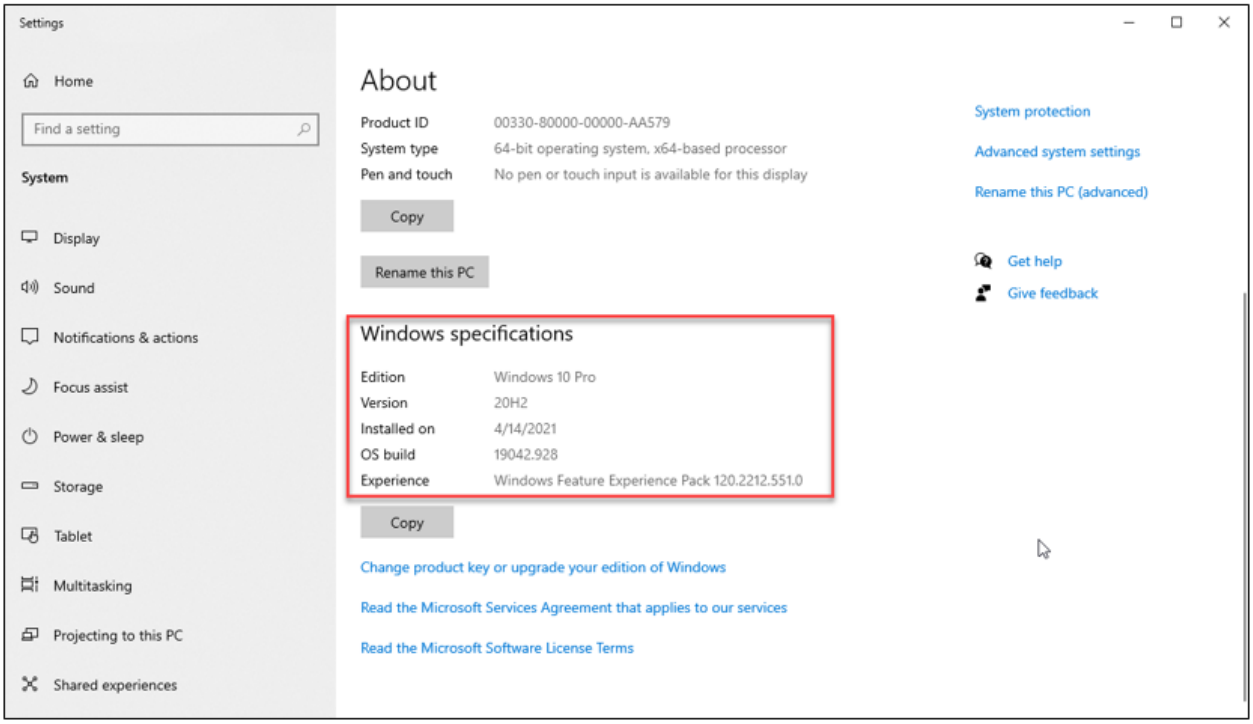
Cách 1: Chọn thanh **Start** > Gõ **winver** > **Enter** để kiểm tra:



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



Kiểm tra mục: **Windows Specifications**

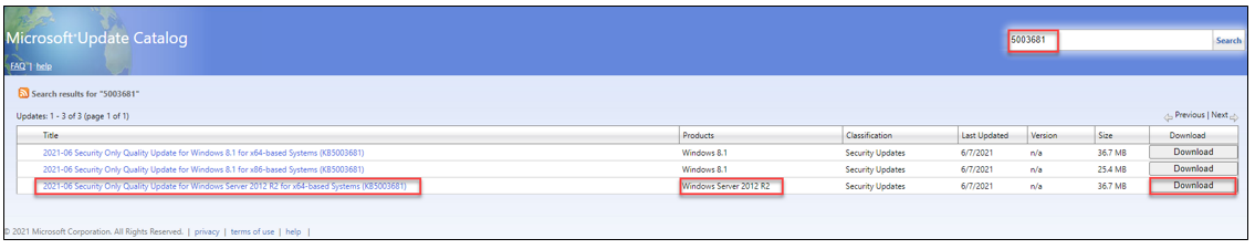


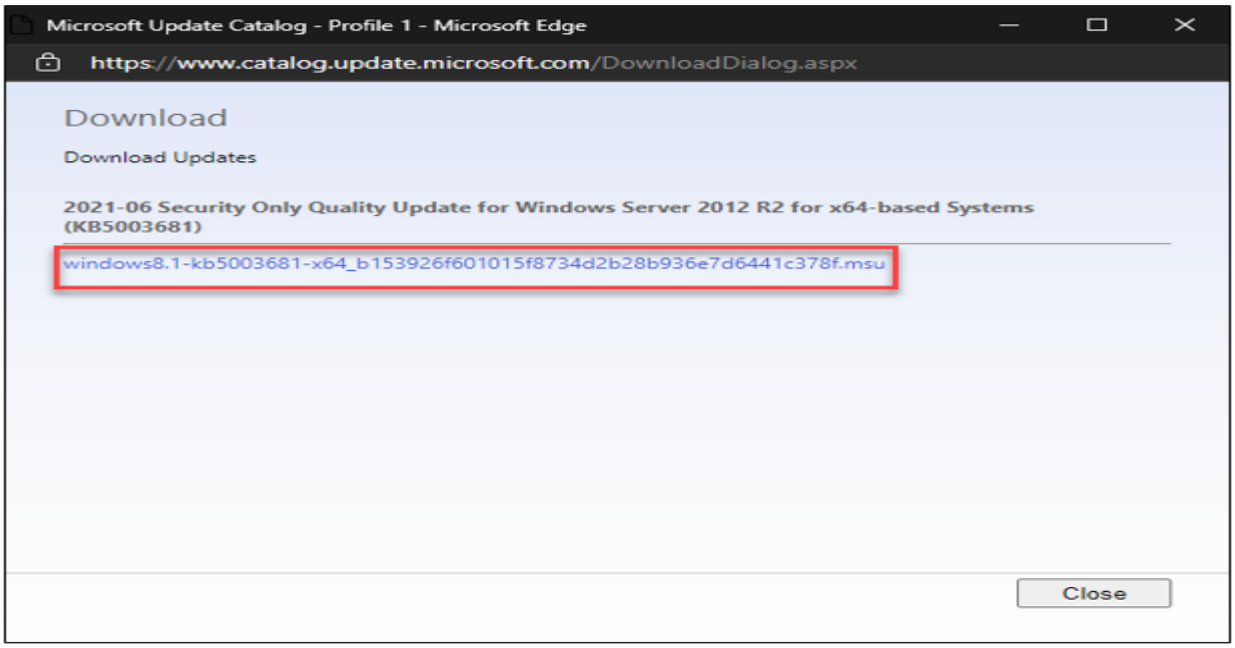
- Bước 2: Download bản vá tại

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

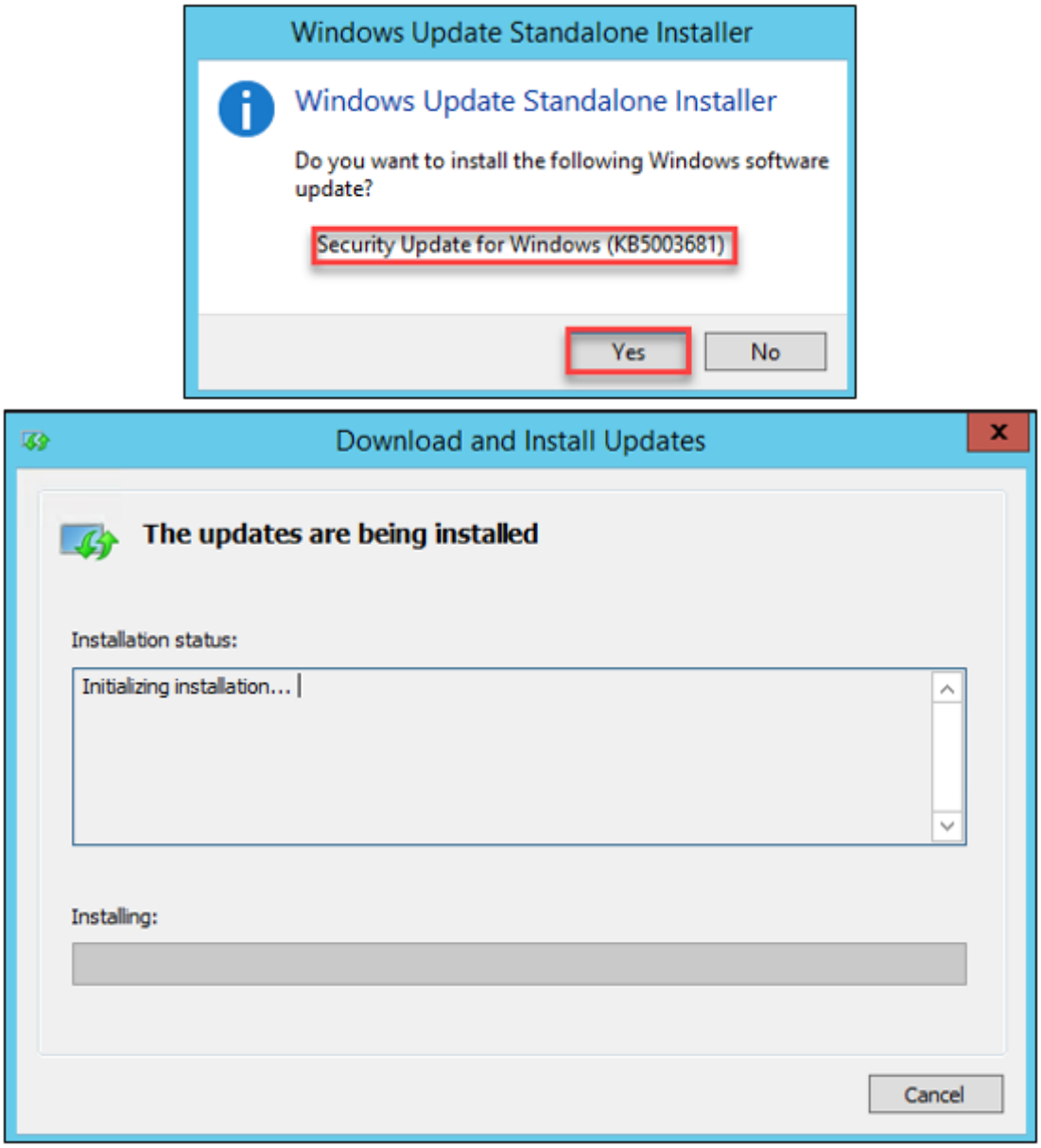
Tại ô **Search** nhập mã **kb** phù hợp dựa vào bảng trên mục **2.1**

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





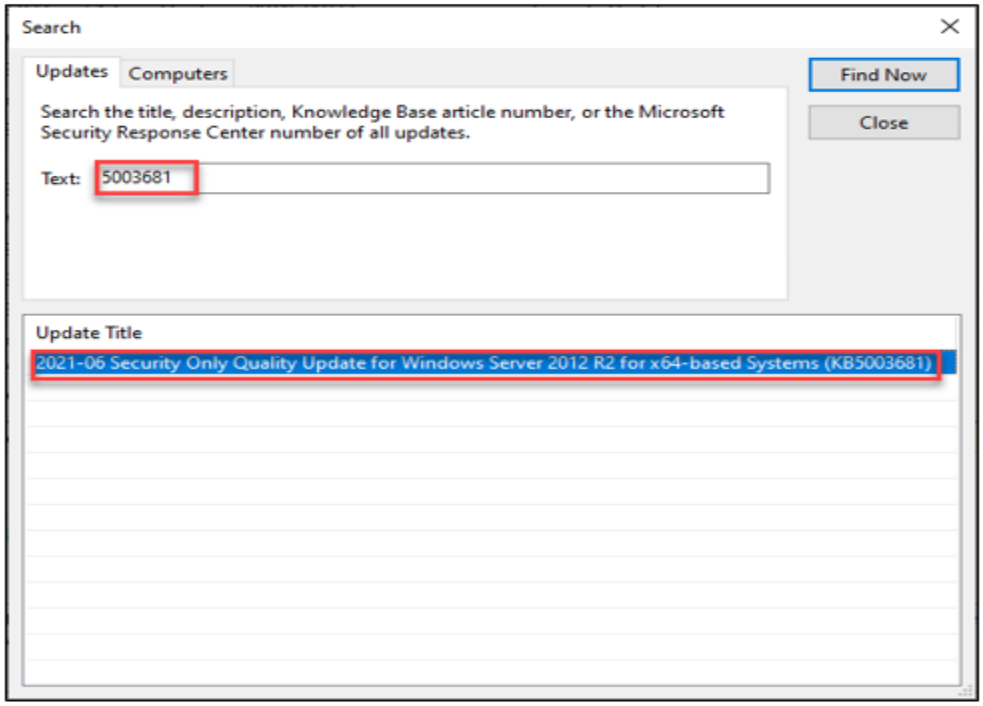
- Bước 4: Cài đặt bản cập nhật đã tải lên từng máy



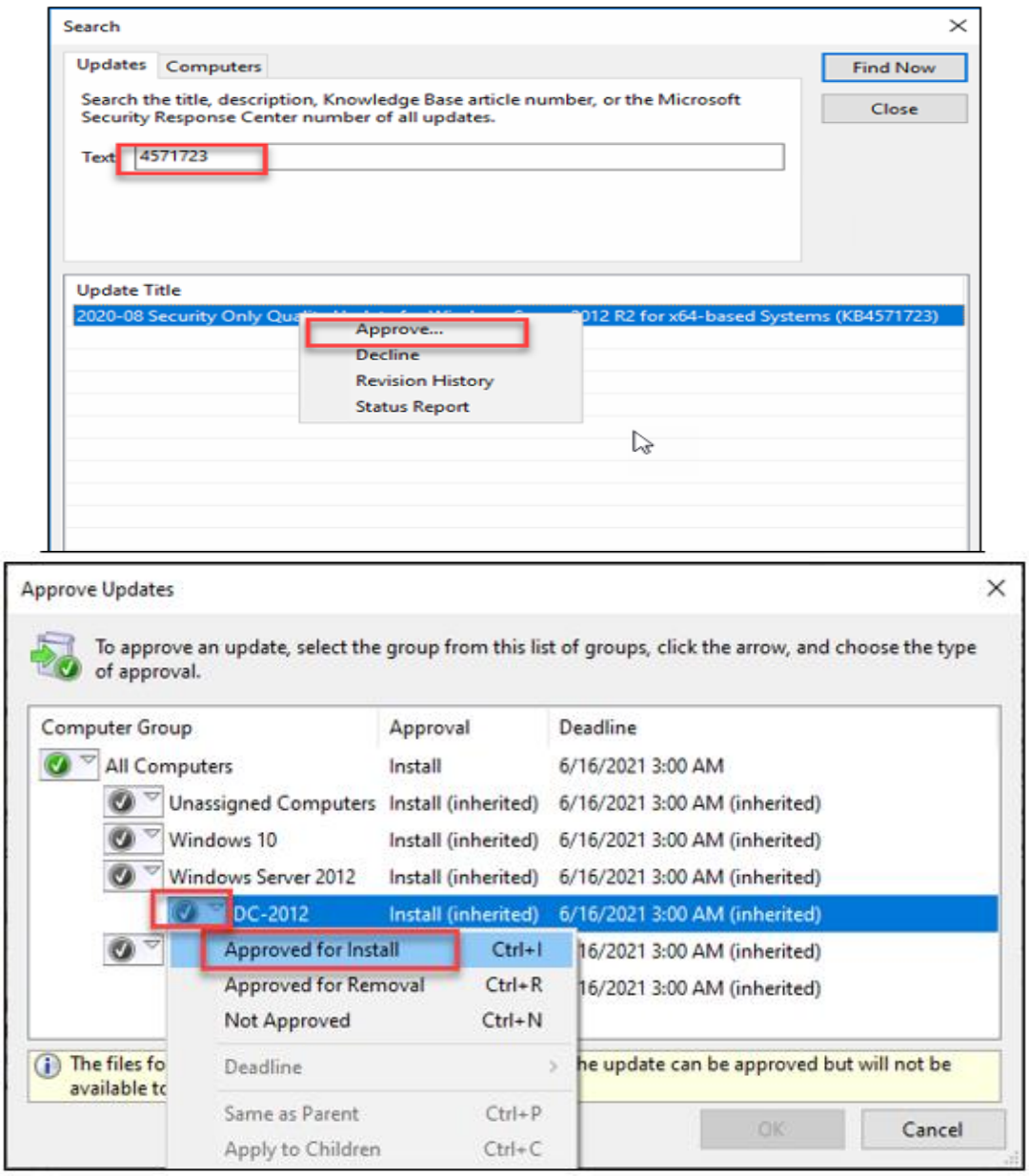
- Bước 5: Khởi động lại máy chủ sau khi tiến hành cài đặt bản cập nhật.

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



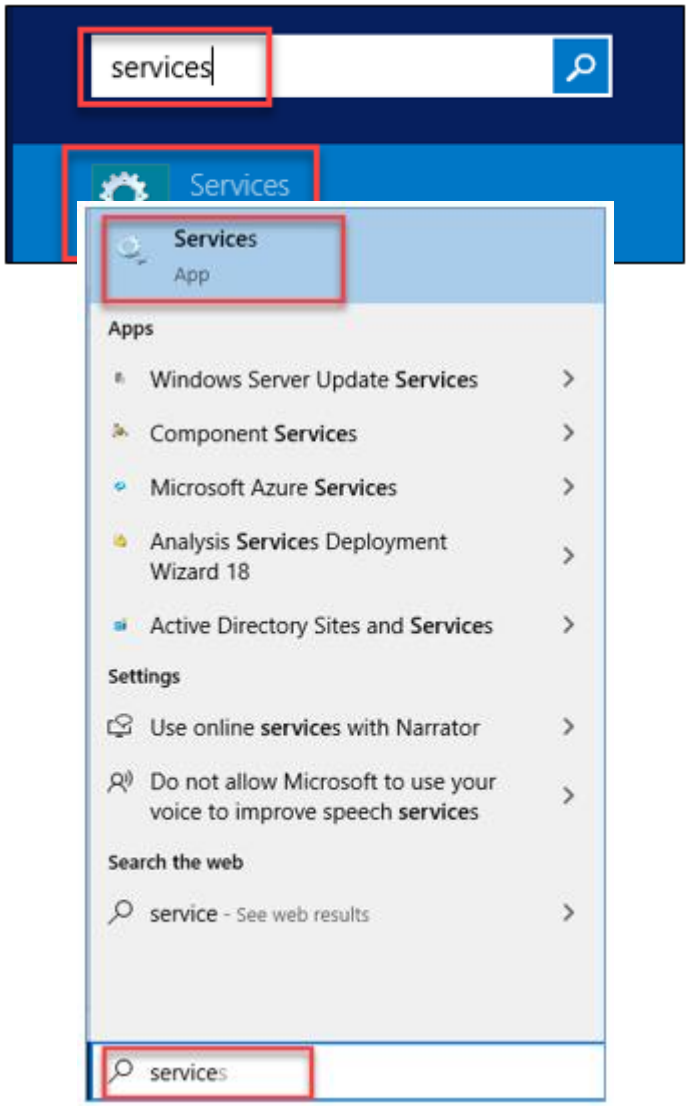
- Bước 3: Cài đặt bản cập nhật và khởi động lại máy chủ.

3.3. Kiểm tra lại bản cài đặt trên máy chủ

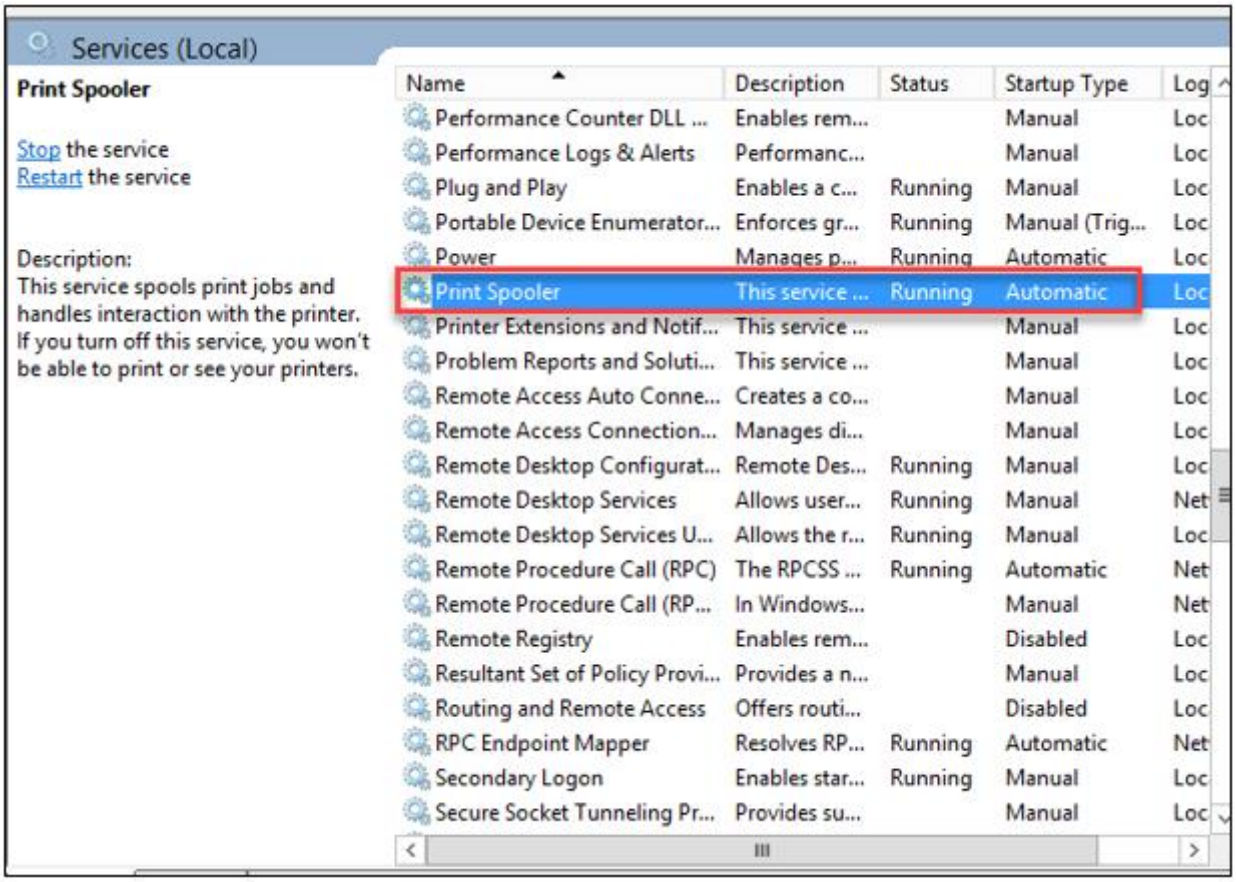
Các bước thực hiện tương tự ở mục **2.2.**

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

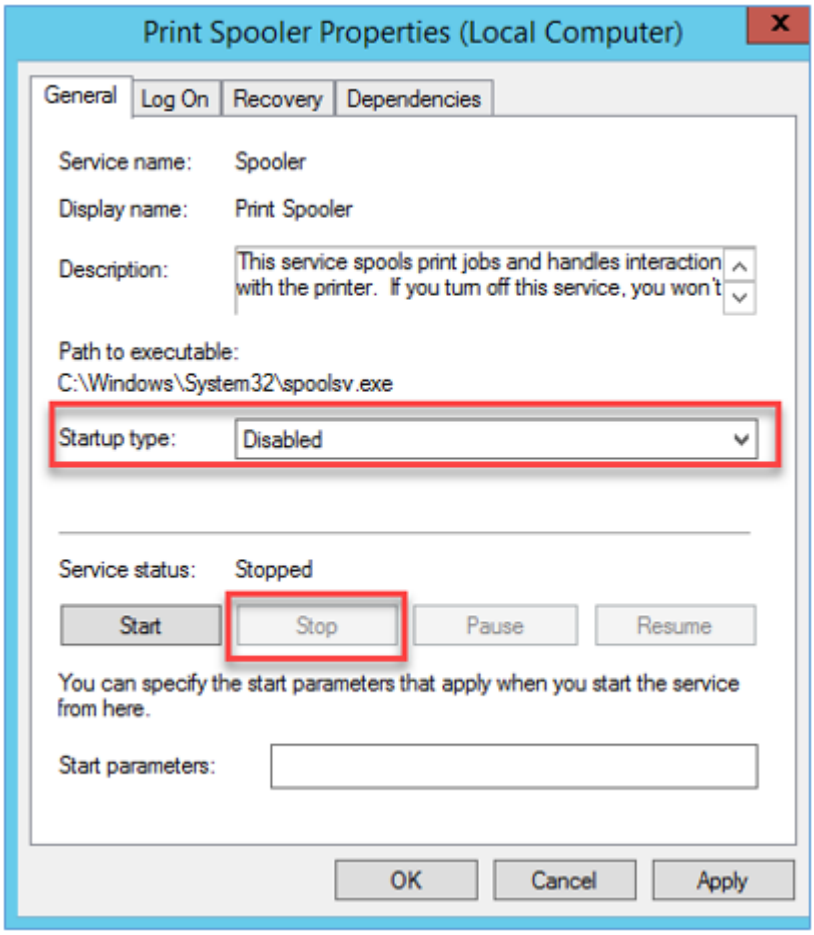
- Bước 1: Vào máy chủ DC, chọn **Start** > Nhập **services.msc** > **Enter**



- 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.