UBND TỈNH THANH HOÁ
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Số: 2760 /STNMT-CNTT

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 3/2023.

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

Thanh Hoá, ngày 04 tháng 4 năm 2023

Kính gửi: Trưởng các đơn vị thuộc Sở

Sở Tài nguyên và Môi trường nhận được Công văn số 62/TTCNTT&TT-QTHT ngày 27/3/2023 của Trung tâm Công nghệ thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2023. Theo đó, có 74 lỗ hổng bảo mật trong các sản phẩm của Microsoft có mức ảnh hưởng cao và nghiêm trọng, cụ thể:

(1) Lỗ hổng bảo mật CVE-2023-23397 (nghiêm trọng) trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế;

(2) Lỗ hổng bảo mật CVE-2023-24880 (trung bình) trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế;

(3) Lỗ hổng bảo mật CVE-2023-23392 (nghiêm trọng) trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa;

(4) Lỗ hổng bảo mật CVE-2023-23415 (nghiêm trọng) trong Internet Control Message Protocol (ICMP) cho phép đối tượng tấn công thực thi mã từ xa;

(5) Lỗ hổng bảo mật CVE-2023-23399 (cao) trong trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa;

(6) Lỗ hổng bảo mật CVE-2023-23400 (cao) trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa;

Để 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. Trưởng các đơn vị trực thuộc Sở thông báo đến toàn thể công chức, viên chức và lao động của đơn vị nghiêm túc thực hiện:

- Kiểm tra, rà soát máy tính cá nhân, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá lỗi kịp thời để tránh nguy cơ bị tấn công (có Hướng dẫn kèm theo).

- 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 (qua 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 Công nghệ thông tin:

- Tổ chức thực hiện rà soát các lỗ hổng nêu trên tại các hệ thống thông tin của Sở Tài nguyên và Môi trường; chủ động vá lỗi, tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

- Chỉ đạo Tổ ứng cứu sự cố Sở, tổ chức hỗ trợ ứng cứu, 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, TTCNTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

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

Lưu Trọng Quang

Phụ lục: Thông tin các lỗ hổng bảo mật

(Kèm theo công văn số /STNMT-CNTT ngày tháng năm 2023 của Sở Tài nguyên và Môi trường)

1. Thông tin các lỗ hổng bảo mật:

STT	CVE	Mô tả	Linh tham khảo
1	CVE-2023-23397	- Điểm: CVSS: 9.1 (nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Outlook, Microsoft Office	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397
2	CVE-2023-24880	- Điểm: CVSS: 5.4 (trung bình) - Mô tả: lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880
3	CVE-2023-23392	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23392
4	CVE-2023-23415	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong Internet Control Message Protocol (ICMP) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415
5	CVE-2023-23399	- Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Microsoft Excel cho phép đối tượng tấn	https://msrc.microsoft.com/update-guide/vulnerability/CVE-

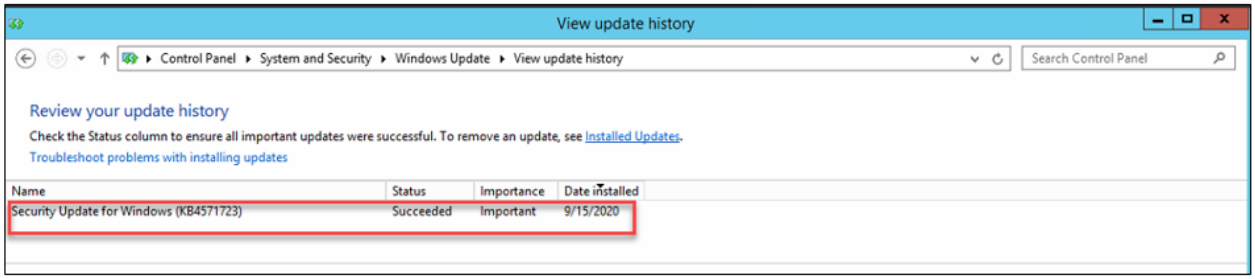
		công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Excel, Microsoft 365 .	2023-23399
6	CVE-2023-23400	- Điểm: CVSS: 7.2 (cao) - Mô tả: lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23400

2. Hướng dẫn khắc phục:

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

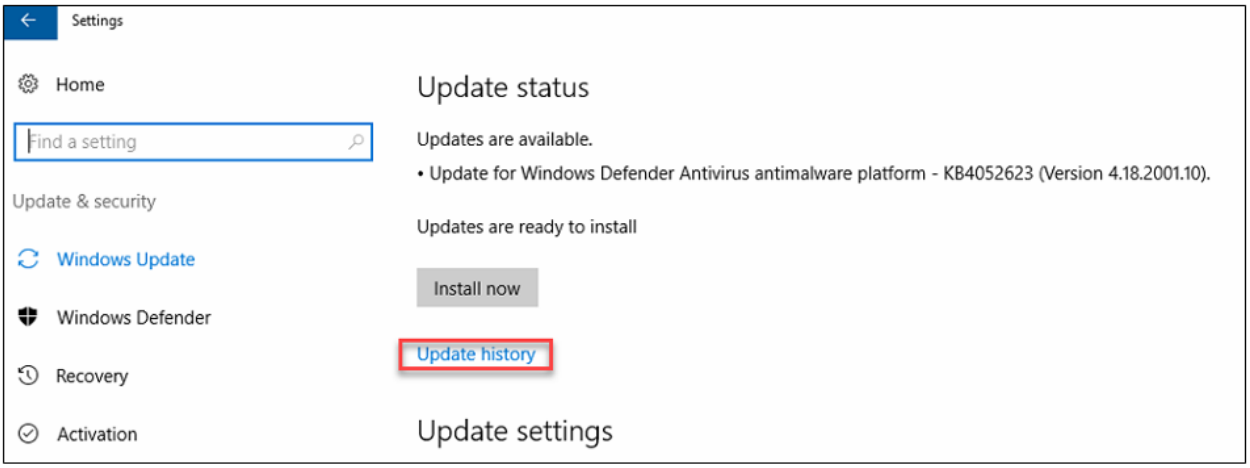
- Windows Server 2012:

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.**



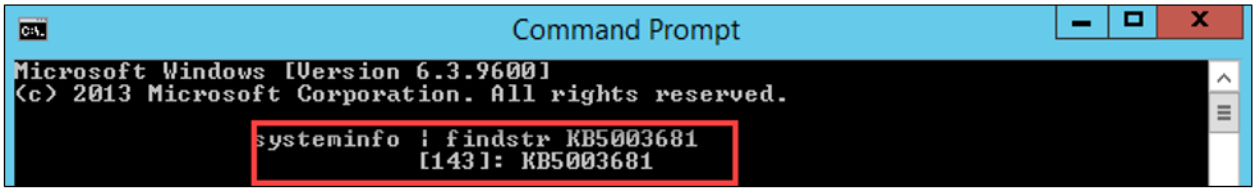
Phương pháp 2: Sử dụng CommandLine

- 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:

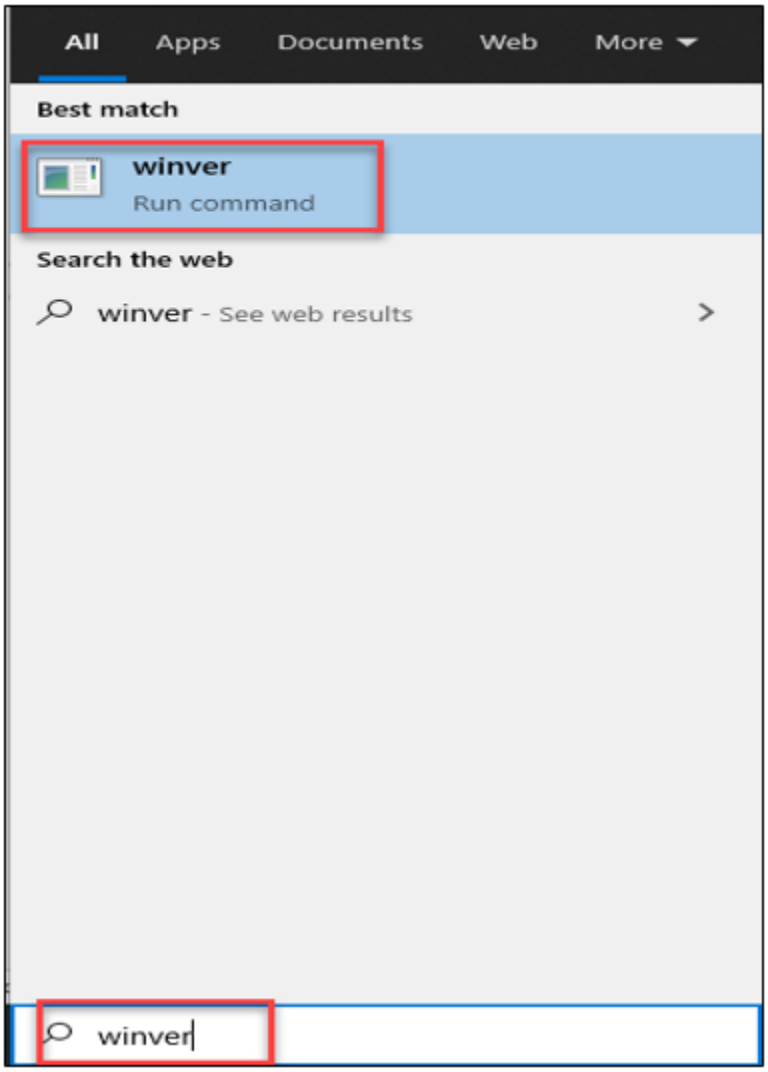


+ Với những máy chủ chưa update, sẽ không hiện ra thông tin:

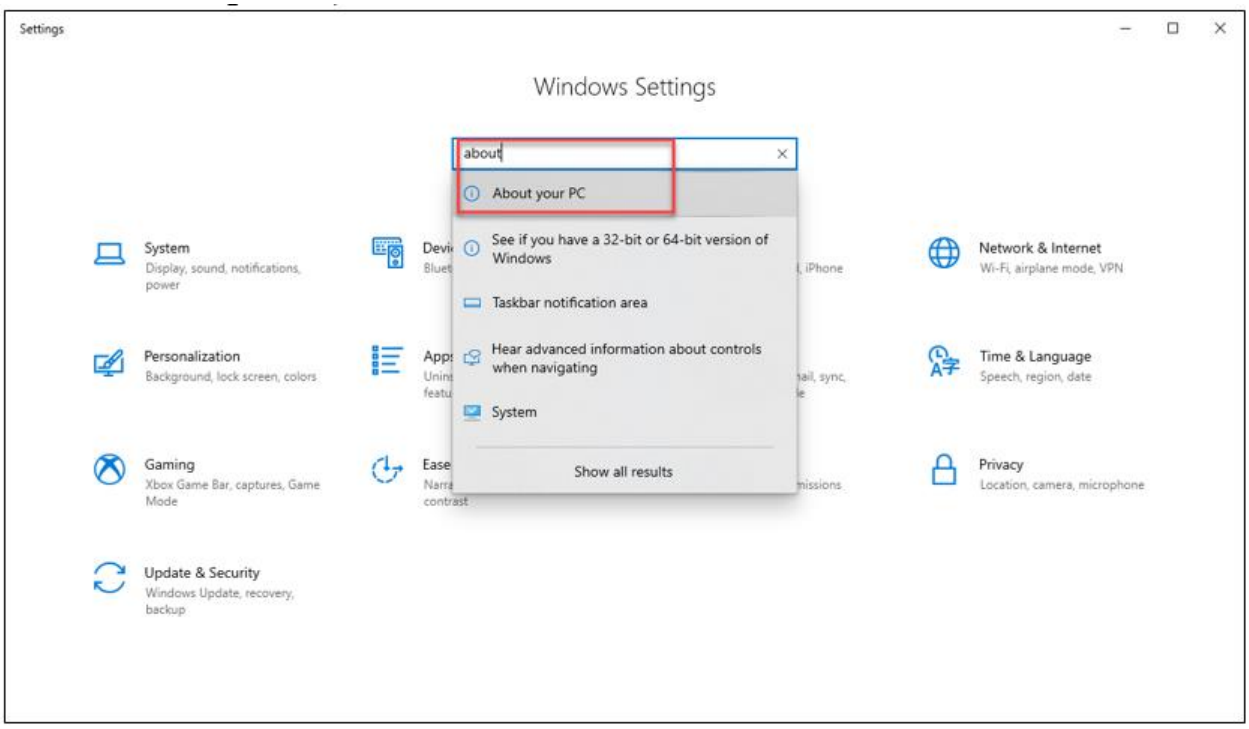
3. Hướng dẫn thực hiện cập nhật bản vá
3.1. Đối với hệ thống không có máy chủ WSUS

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

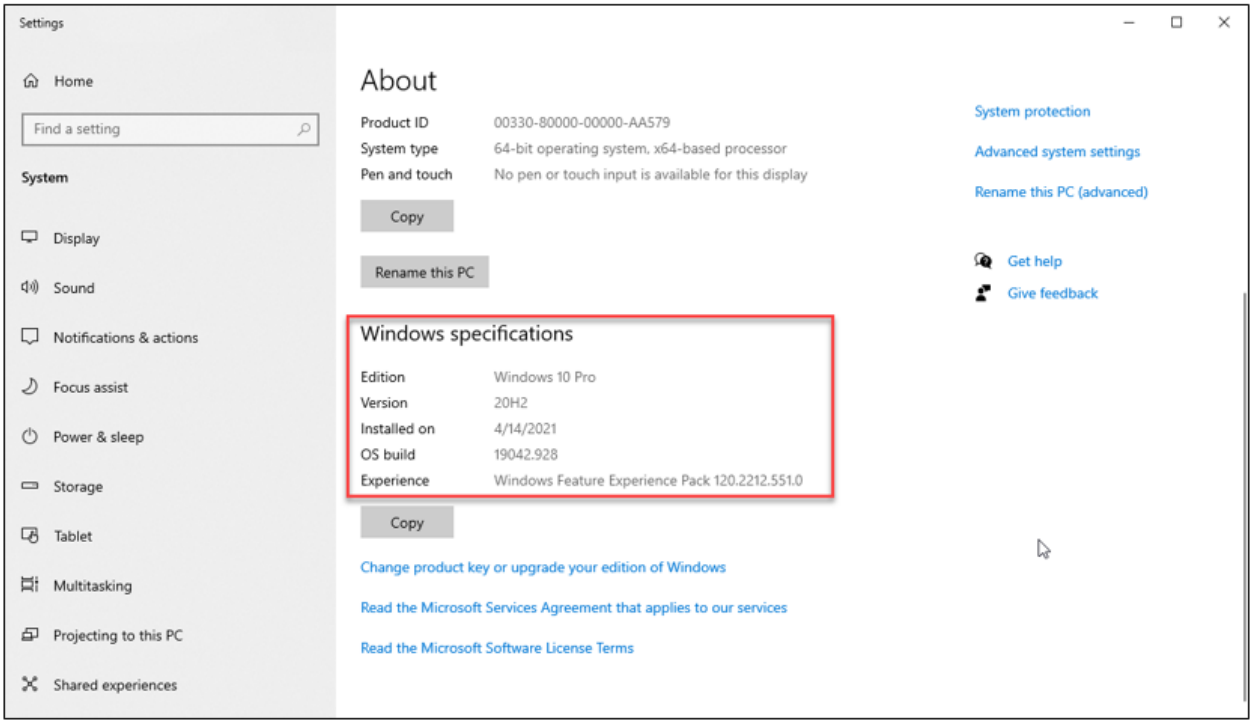
Cách 1: Chọn thanh **Start** > Gõ **winver** > **Enter** để kiểm tra:



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



Kiểm tra mục: **Windows Specifications**

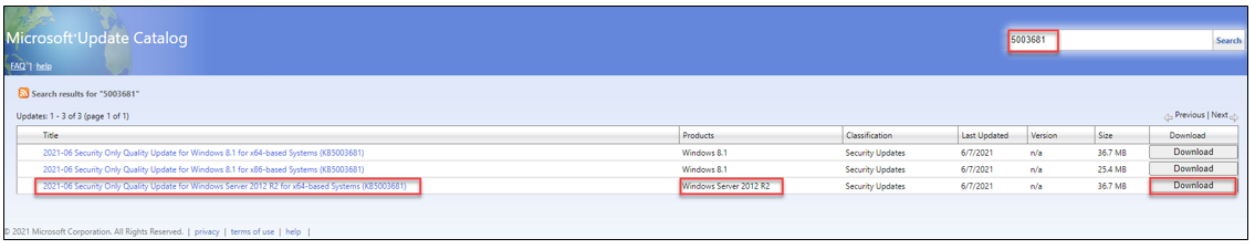


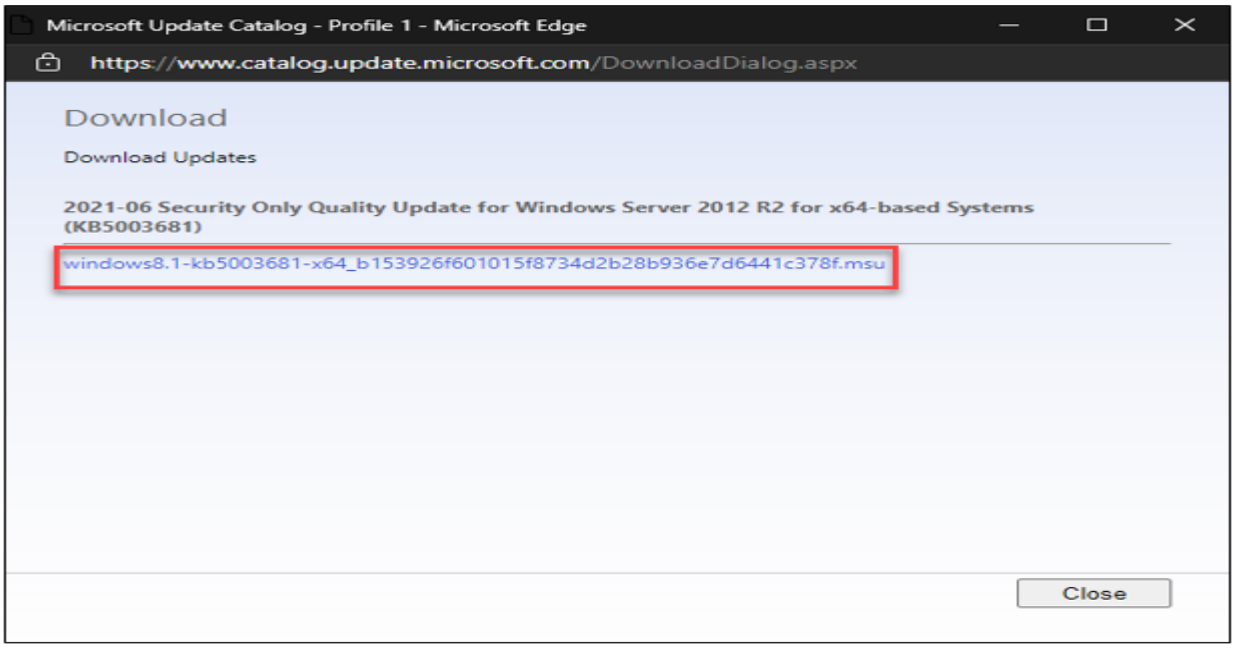
- Bước 2: Download bản vá tại

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

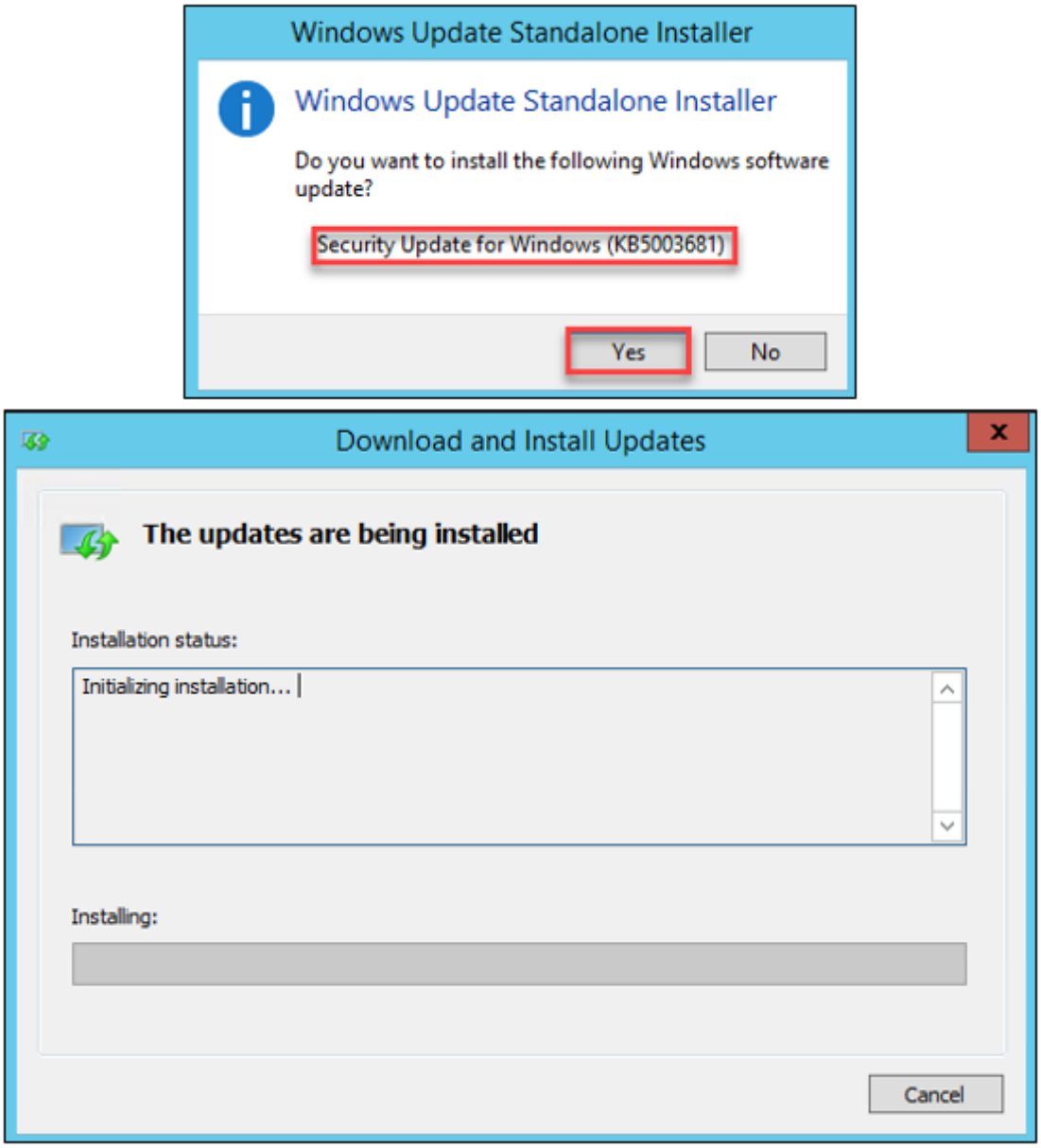
Tại ô **Search** nhập mã **kb** phù hợp dựa vào bảng trên mục **2.1**

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





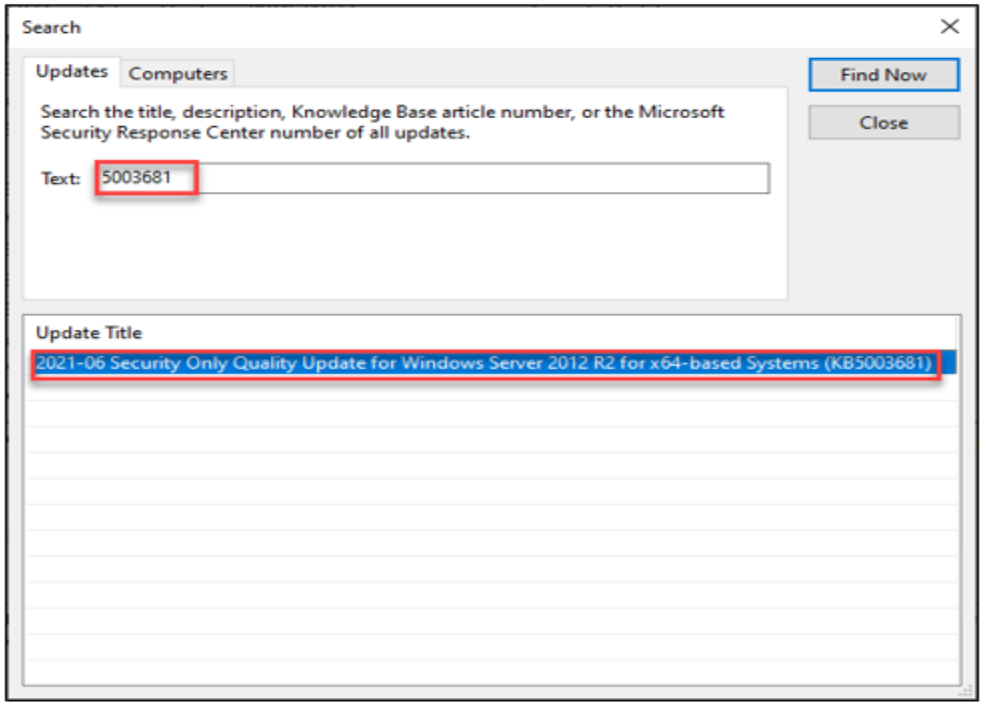
- Bước 4: Cài đặt bản cập nhật đã tải lên từng máy



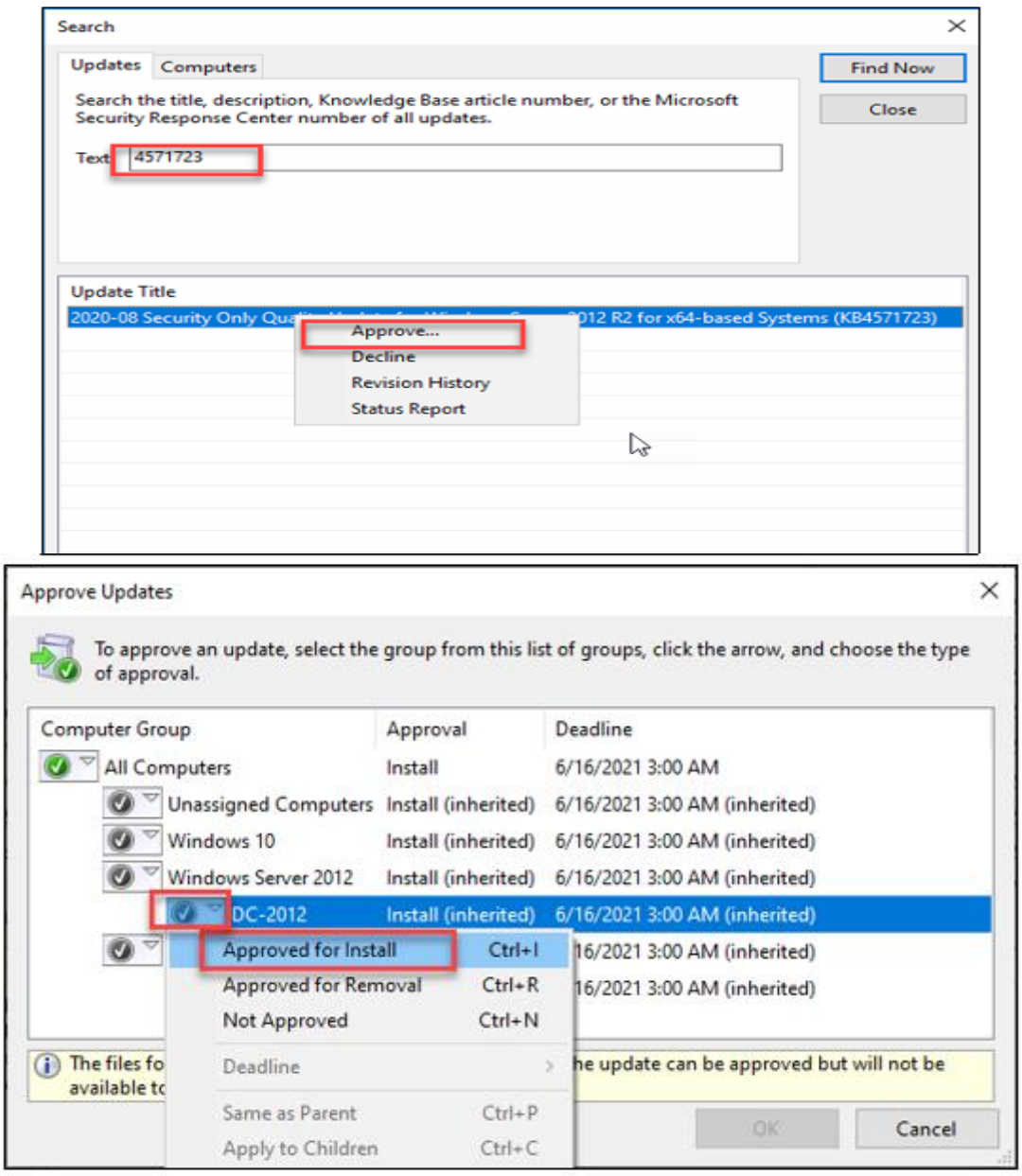
- Bước 5: Khởi động lại máy chủ sau khi tiến hành cài đặt bản cập nhật.

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



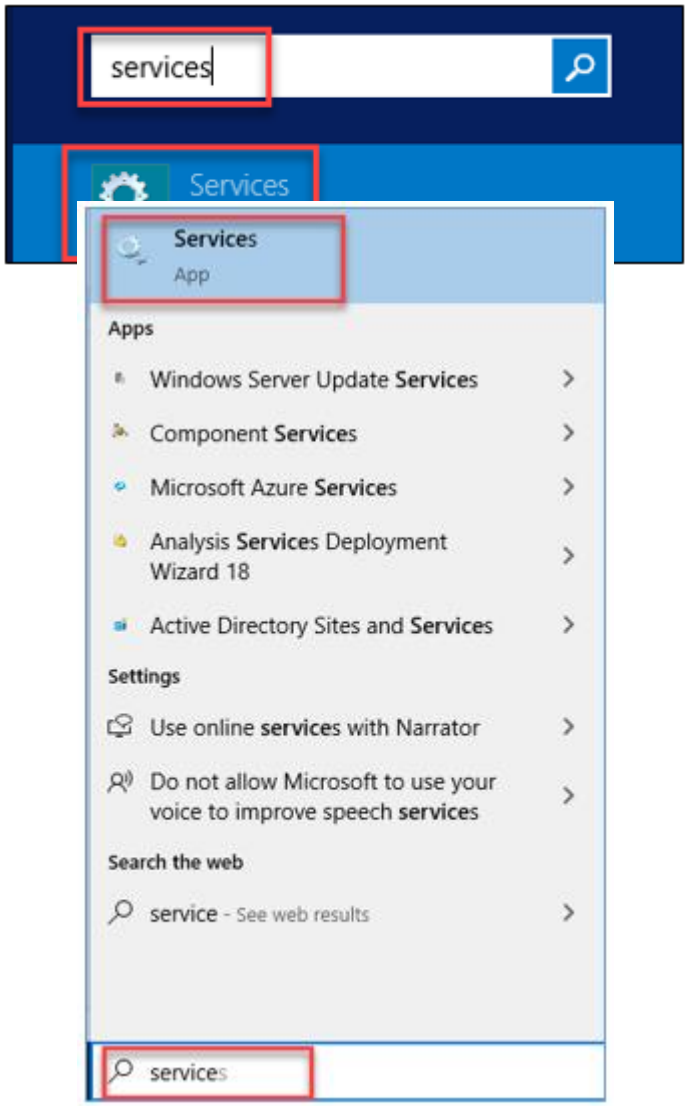
- Bước 3: Cài đặt bản cập nhật và khởi động lại máy chủ.

3.3. Kiểm tra lại bản cài đặt trên máy chủ

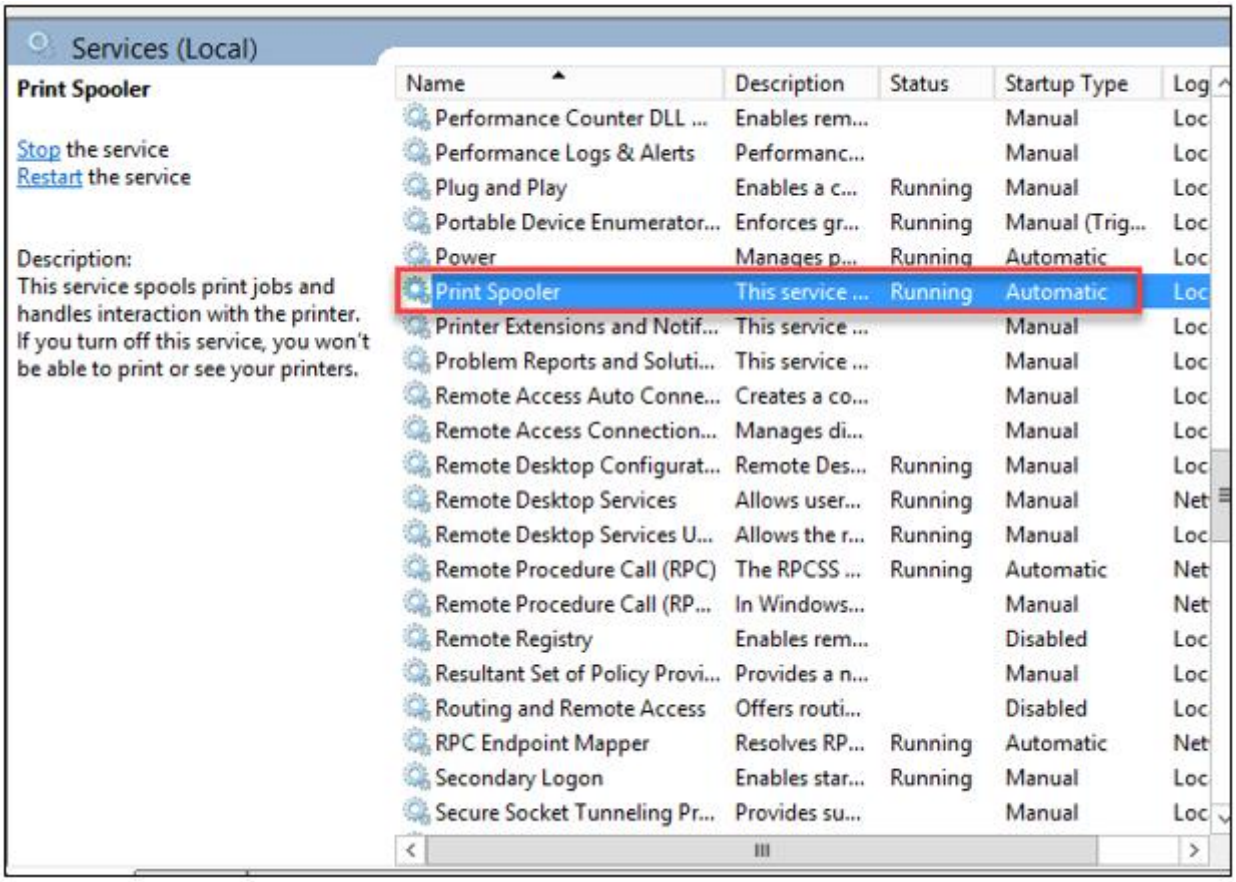
Các bước thực hiện tương tự ở mục **2.2.**

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

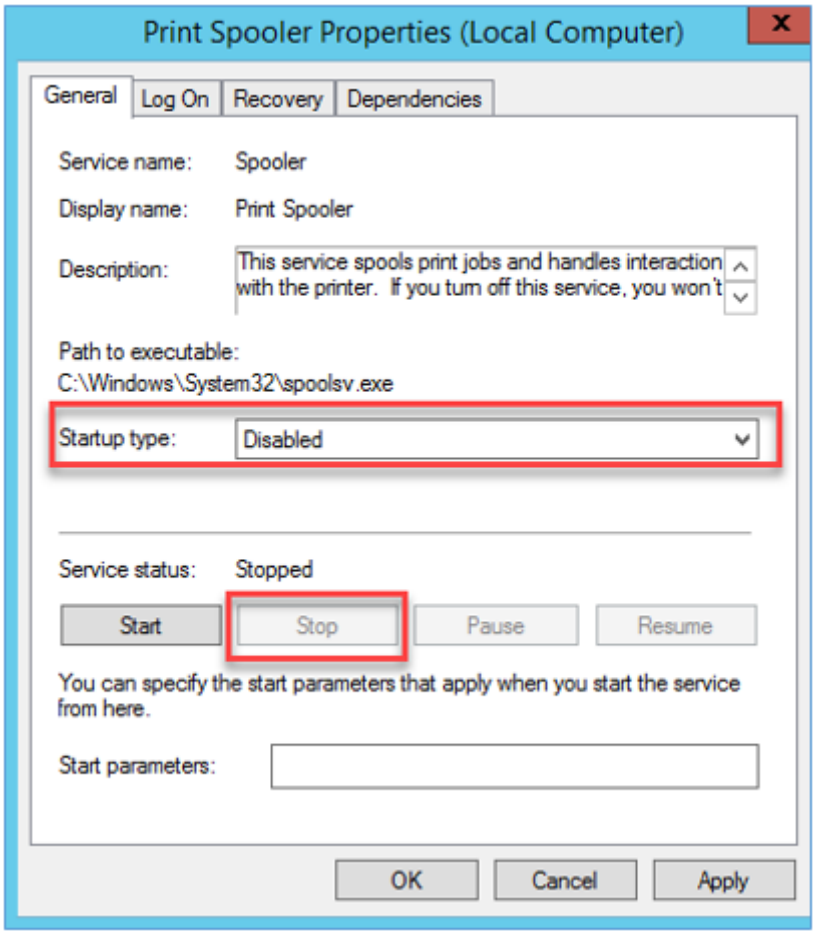
- Bước 1: Vào máy chủ DC, chọn **Start** > Nhập **services.msc** > **Enter**



- 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.