UBND TỈNH SƠN LA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 800 /STTTT-CNTT
V/v Cảnh báo nguy cơ tấn công mạng vì lỗ hổng Windows

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

Sơn La, ngày 02 tháng 7 năm 2021

Kính gửi:
- Văn phòng tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các Sở, ban, ngành;
- Mặt trận tổ quốc và các Đoàn thể của tỉnh;
- Công an tỉnh Sơn La;
- Ban Chỉ huy quân sự tỉnh Sơn La;
- UBND các huyện, thành phố;
- Trung tâm Công nghệ thông tin và Truyền thông;

Mới đây, Microsoft đã công bố về lỗ hổng bảo mật có mã **CVE-2021-1675** trên hệ điều hành Windows có mức độ nguy hiểm cao (7.8/10). Lỗ hổng này ảnh hưởng đến hầu hết các phiên bản của hệ điều hành Windows, bao gồm: Windows 10/8.1/7, Windows Server 2019/2016/2012/2008.

CVE-2021-1675 tồn tại trong Windows Print Spooler, cho phép các đối tượng tấn công leo thang đặc quyền từ tài khoản người dùng thông thường có rất ít quyền. Vào ngày 8/6 vừa qua, Microsoft đã phát hành bản vá cho lỗ hổng bảo mật này. Tuy nhiên, theo phân tích và đánh giá từ Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã ghi nhận một số thông tin bổ sung mới cho thấy lỗ hổng bảo mật **CVE-2021-1675** có mức độ nguy hiểm cao hơn thực tế được công bố.

Nếu khai thác thành công lỗ hổng này, kẻ xấu không chỉ khai thác được khi có quyền truy cập trực tiếp vào máy tính, máy chủ cài đặt phiên bản hệ điều hành Windows mà còn có thể tấn công thông qua một mạng máy tính. Thực hiện nhiệm vụ là cơ quan chuyên trách về công nghệ thông tin và thành viên của mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia; Để tránh trở thành nạn nhân của hình thức tấn công nói trên, Sở Thông tin và Truyền thông khuyến nghị:

1. Thủ trưởng các cơ quan, đơn vị nghiêm túc quán triệt, chỉ đạo các cán bộ, công chức, viên chức, người lao động thực hiện một số biện pháp sau:

- Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi lỗ hổng **CVE-2021-1675**. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo hướng dẫn của Microsoft (*hướng dẫn chi tiết tham khảo tại phụ lục kèm theo*).

- Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

- 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.

2. Trung tâm Công nghệ thông tin và Truyền thông thực hiện rà soát, kiểm tra, cập nhật, triển khai các biện pháp đảm bảo an toàn cho hệ thống máy chủ tại Trung tâm.

Đầu mối hỗ trợ:

- Bộ Thông tin và Truyền thông: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, điện thoại: 02432091616, thư điện tử: ais@mic.gov.vn

- Sở Thông tin và Truyền thông:

+ Phòng Công nghệ thông tin, điện thoại: 02122210468.

+ Trung tâm Công nghệ thông tin và Truyền thông, điện thoại: 02123858728

Đề nghị các cơ quan, đơn vị quan tâm, thực hiện./.

Nơi nhận:
- Như trên;
- Thường trực UBND tỉnh (để báo cáo);
- Báo Sơn La; Đài PT-TH tỉnh;
- Ban Giám đốc;
- Lưu VT, CNTT (Tr 39b).

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH SƠN LA

Phạm Quốc Chinh

PHỤ LỤC

THÔNG TIN LỖ HỔNG BẢO MẬT

1. Thông tin lỗ hổng bảo mật (CVE-2021-1675)

- Mô tả: Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công leo thang đặc quyền chỉ với quyền người dùng thấp.

- Điểm CVSS: 7.8 (cao)

- Ảnh hưởng: hầu hết các phiên bản hệ điều hành Windows. Thông tin chi tiết các phiên bản tham khảo tại: https://msrc.microsoft.com/update-guide/enUS/vulnerability/CVE-2021-1675

Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục lỗ hổng bảo mật này là cập nhật bản vá. Do trong thời điểm hiện tại, Microsoft chưa có thông tin về các biện pháp giảm thiểu thay thế.

2.1. Bảng mã cập nhật cần tải cho từng phiên bản hệ điều hành

TT	Hệ điều hành	Mã kb	Ghi chú
1	Windows Server 2008 R2 for x64-based Systems Service Pack 1	5003667	Bản update tháng
		5003694	Bản update security
2	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5003667	Bản update tháng
		5003694	Bản update security
3	Windows Server 2012	5003697	Bản update tháng
		5003696	Bản update security
4	Windows Server 2012 (Server Core installation)	5003697	Bản update tháng
		5003696	Bản update security

5	Windows Server 2012 R2	5003671	Bản update tháng
		5003681	Bản update security
6	Windows Server 2012 R2 (Server Core installation)	5003671	Bản update tháng
		5003681	Bản update security
7	Windows Server 2016	5003638	Bản update security
8	Windows Server 2016 (Server Core installation)	5003638	Bản update security
9	Windows Server 2019	5003646	Bản update security
10	Windows Server 2019 (Server Core installation)	5003646	Bản update security
11	Windows Server, version 2004 (Server Core installation)	5003637	Bản update security
12	Windows Server, version 20H2 (Server Core installation)	5003637	Bản update security
13	Windows 10 Version 1607 (32-bit Systems/x64-based Systems)	5003638	Bản update security
14	Windows 10 Version 1809 (32-bit Systems/ARM64-based Systems/x64-based Systems)	5003646	Bản update security
15	Windows 10 Version 1909 (32-bit Systems/ARM64-based Systems/x64-based Systems)	5003635	Bản update security
16	Windows 10 Version 2004 (32-bit Systems/ARM64-based Systems/x64-based Systems)	5003637	Bản update security
17	Windows 10 Version 20H2 (32-bit Systems/ARM64-based Systems/x64-based Systems)	5003637	Bản update security
18	Windows 10 Version 21H1 (32-bit Systems/ARM64-based Systems/x64-based Systems)	5003637	Bản update security
19	Windows 10 (32-bit Systems/ x64-based Systems)	5003687	Bản update security
20	Windows 7 (32-bit System) Service Pack 1	5003667	Bản update tháng
		5003694	Bản update security

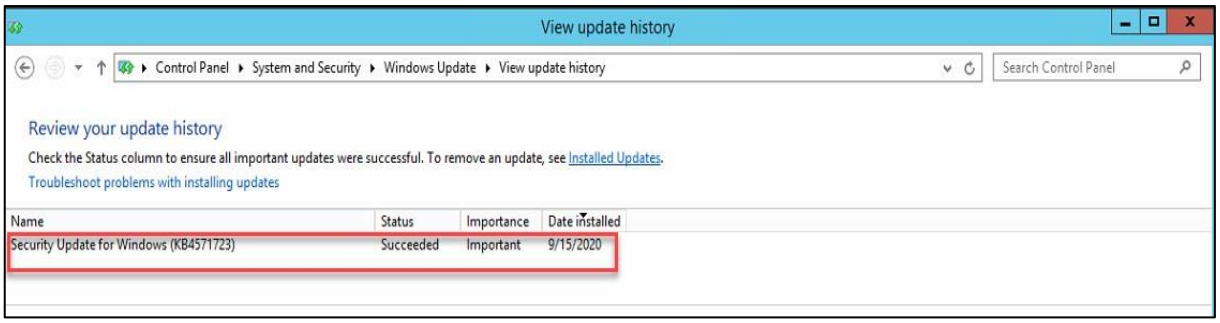
21	Windows 7 (x64-based System) Service Pack 1	5003667	Bản update tháng
		5003694	Bản update security
22	Windows 8.1 (32-bit Systems)	5003671	Bản update tháng
		5003681	Bản update security
23	Windows 8.1 (x64-based Systems)	5003671	Bản update tháng
		5003681	Bản update security
24	Windows RT 8.1	5003671	Bản update tháng

2.2. Hướng dẫn kiểm tra lịch sử cập nhật

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

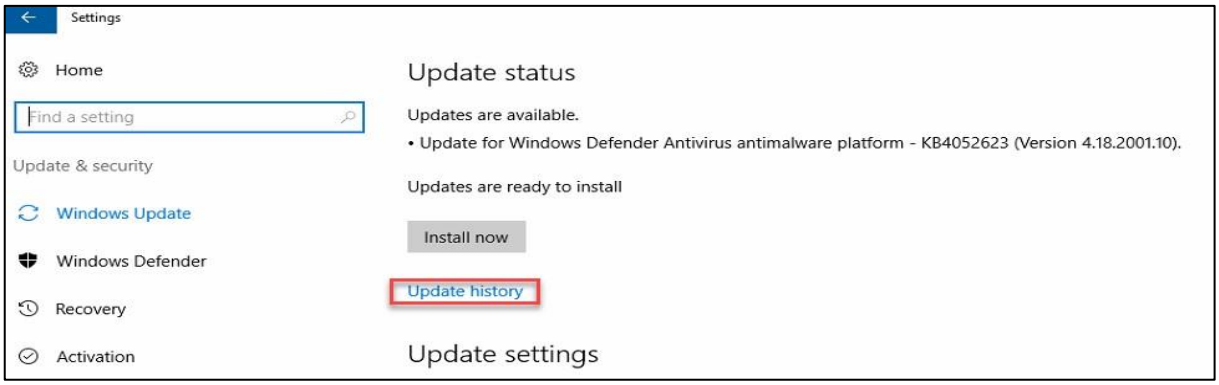
- Windows Server 2012:

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:

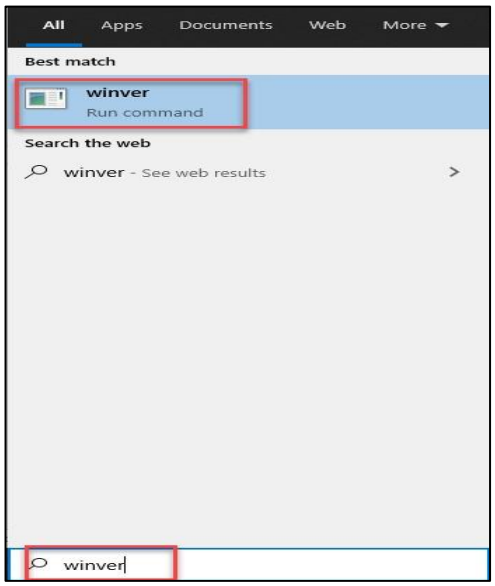
+ Với những máy chủ chưa update, sẽ không hiện ra thông tin:

2.3. Hướng dẫn thực hiện cập nhật bản vá

2.3.1. Đối với hệ thống không có máy chủ WSUS *(Là các máy trạm hoạt động riêng rẽ, không có có máy chủ quản lý tập trung)*

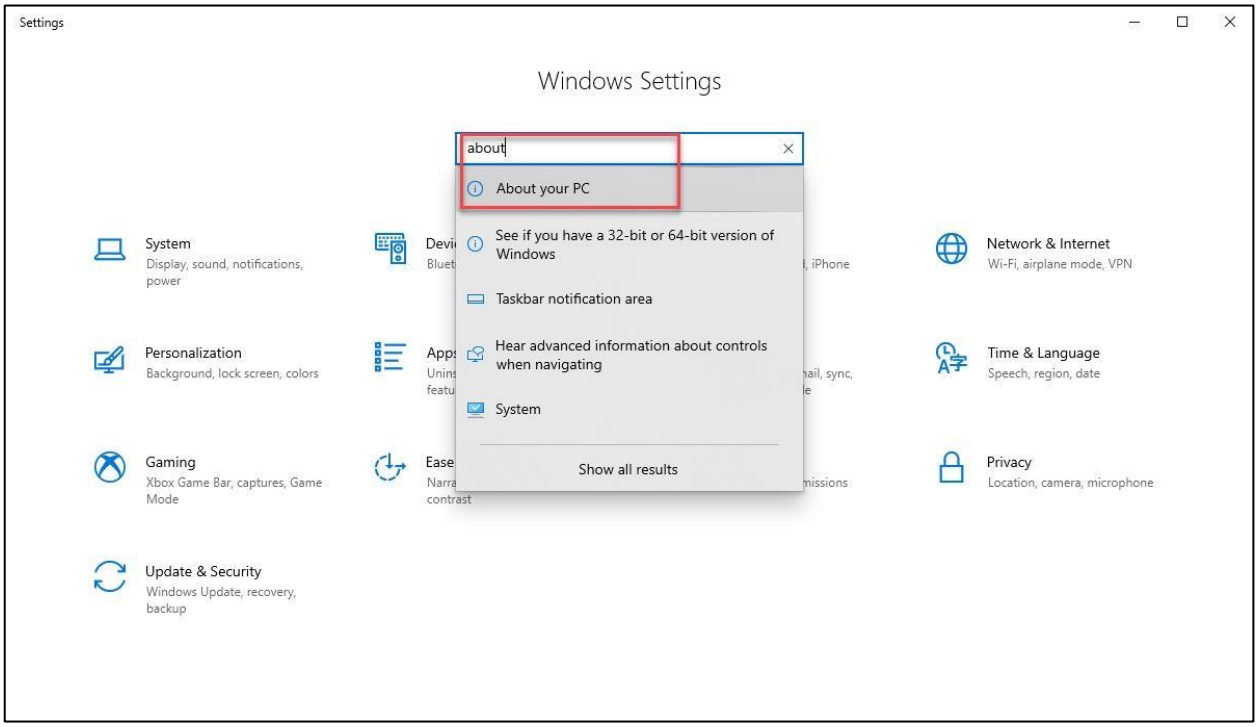
- Bước 1: Kiểm tra OS, version hệ điều hành đang sử dụng:

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

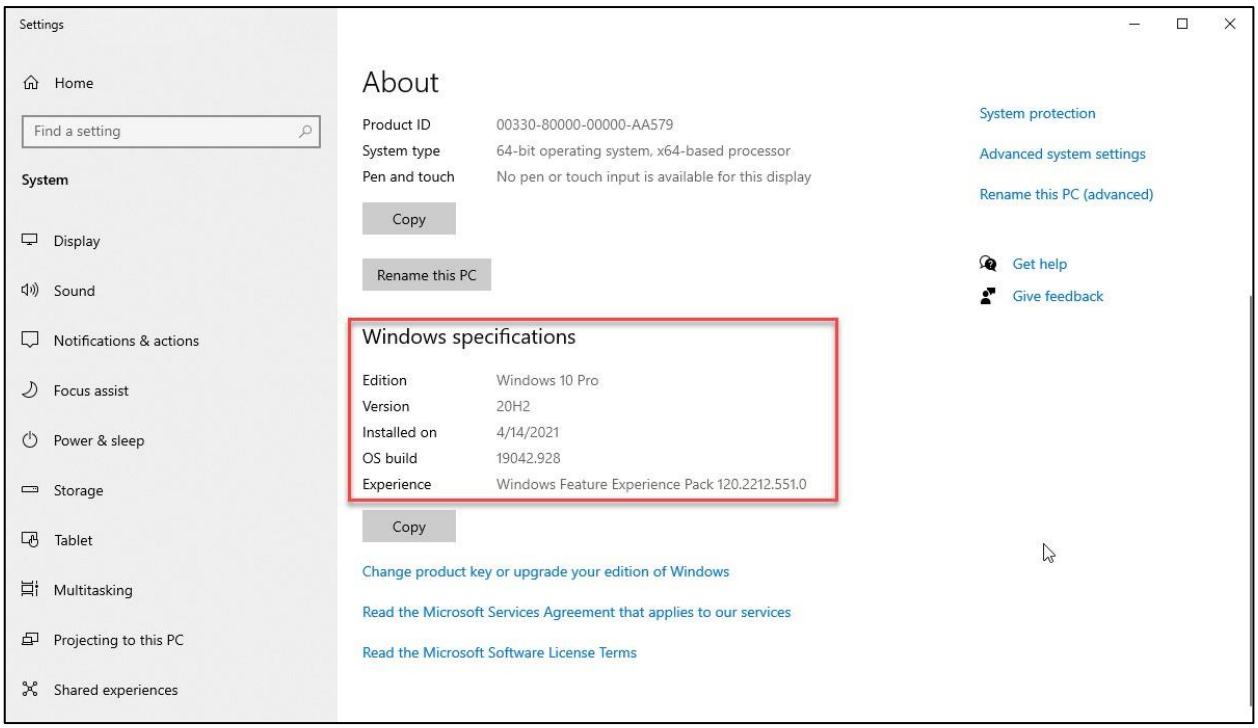


<u>Cách 2:</u> Chọn **Setting** > Nhập ô tìm kiếm "**About this PC**" (hoặc chuột phải

This PC > **Properties**)



Kiểm tra mục: ***Windows Specifications***

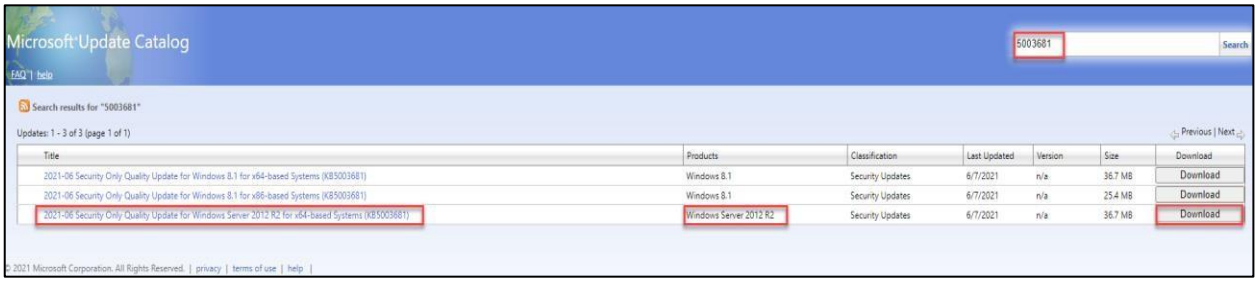


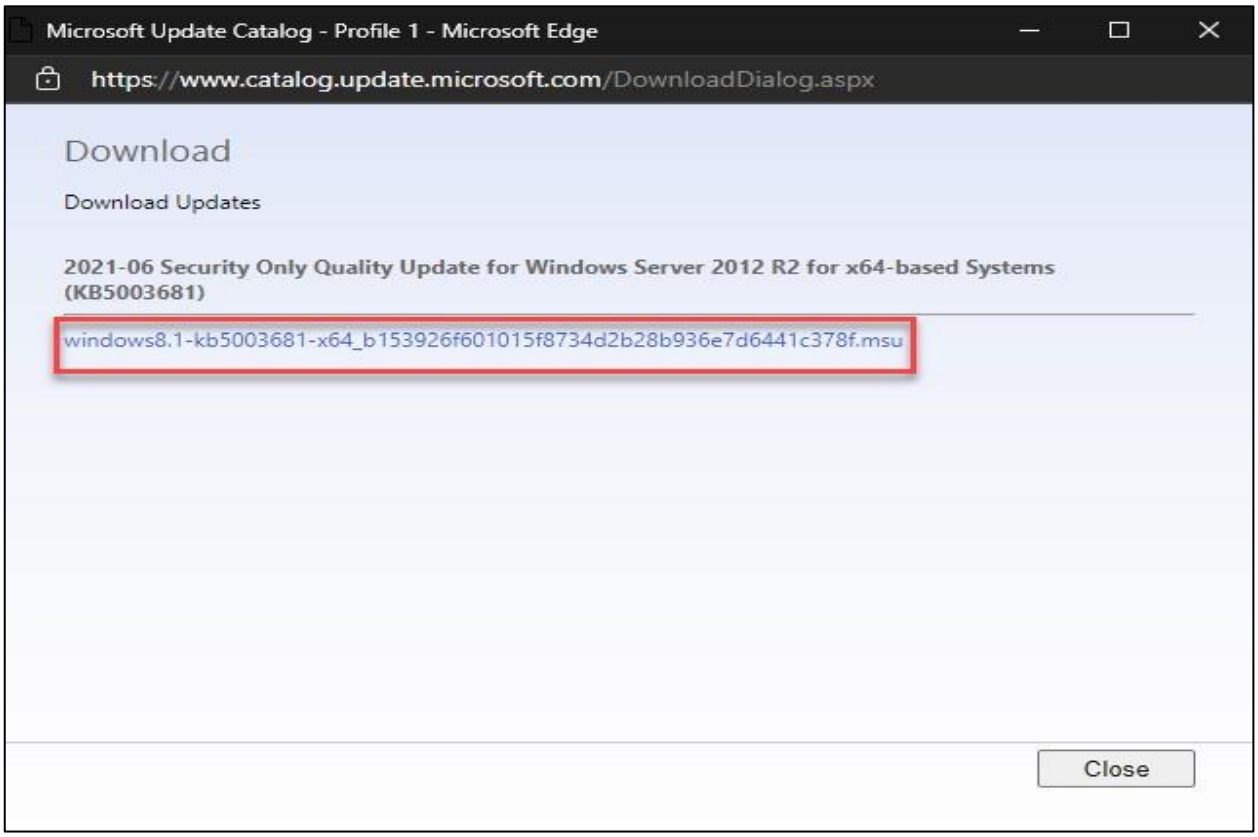
Bước 2: Download bản vá tại

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

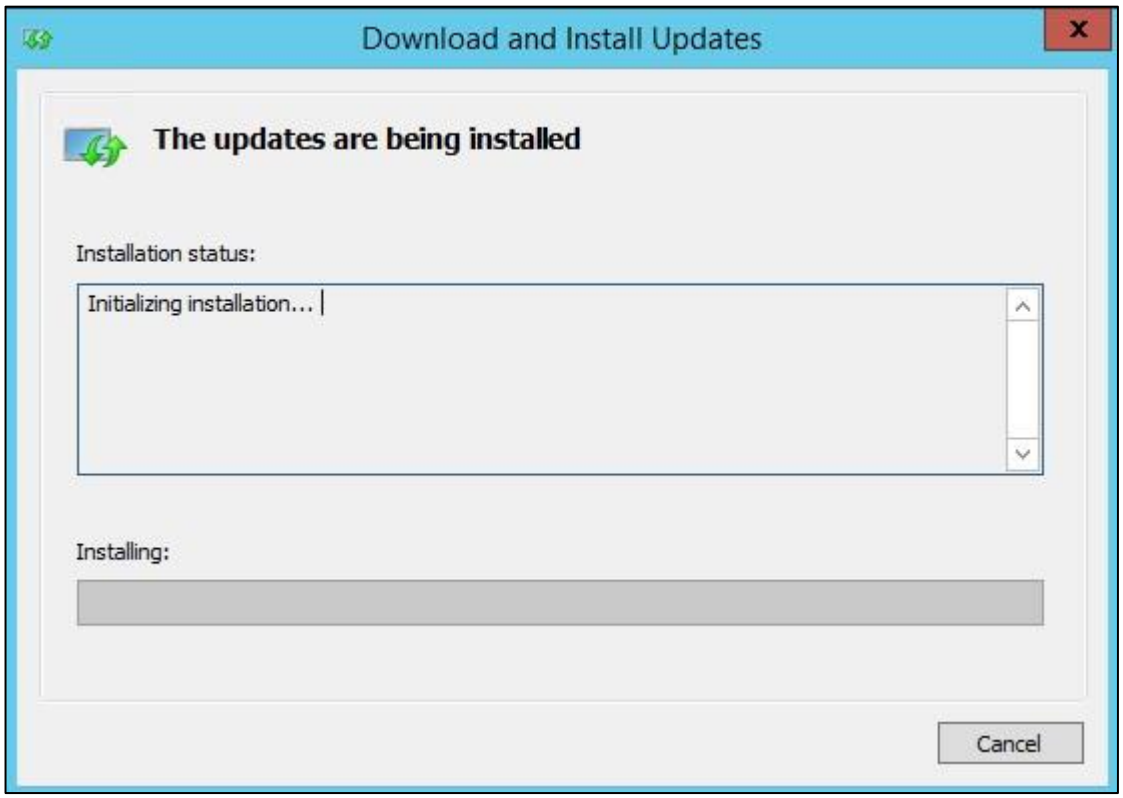
Tại ô **Search** nhập mã **kb** phù hợp dựa vào bảng trên **mục 2.1**

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





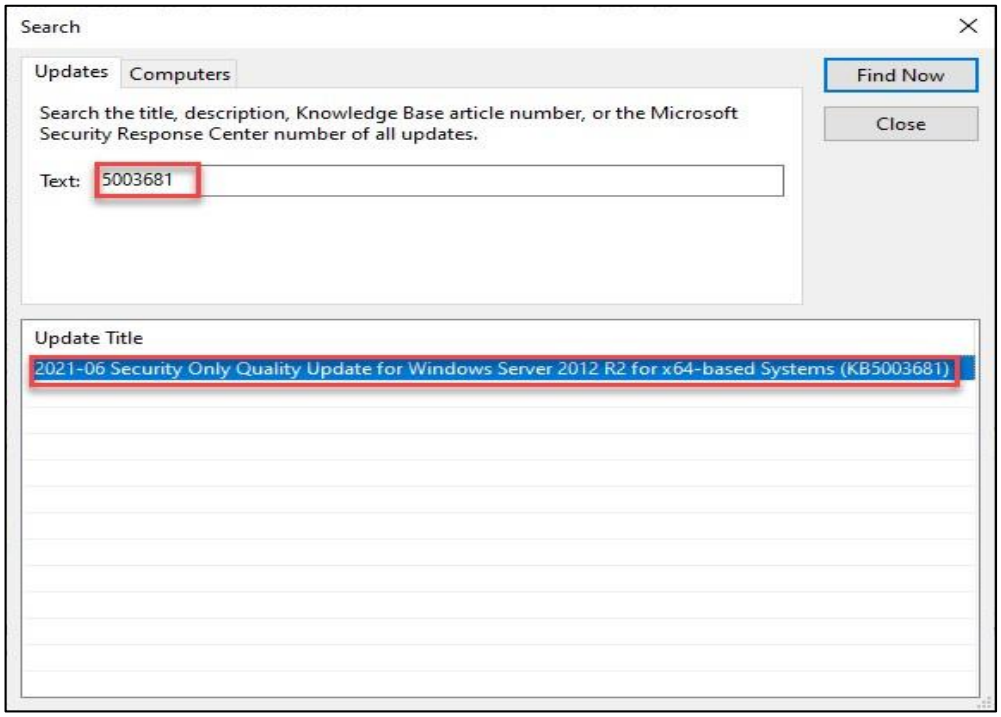
- Bước 4: Cài đặt bản cập nhật đã tải lên từng máy



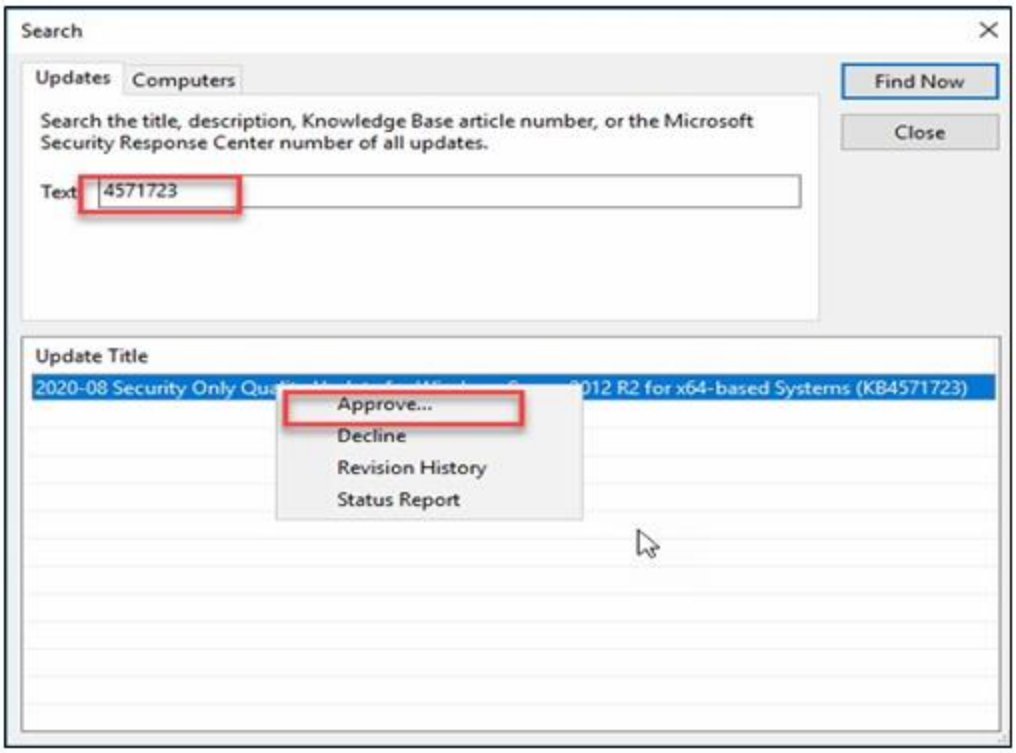
- Bước 5: Khởi động lại máy chủ sau khi tiến hành cài đặt bản cập nhật.

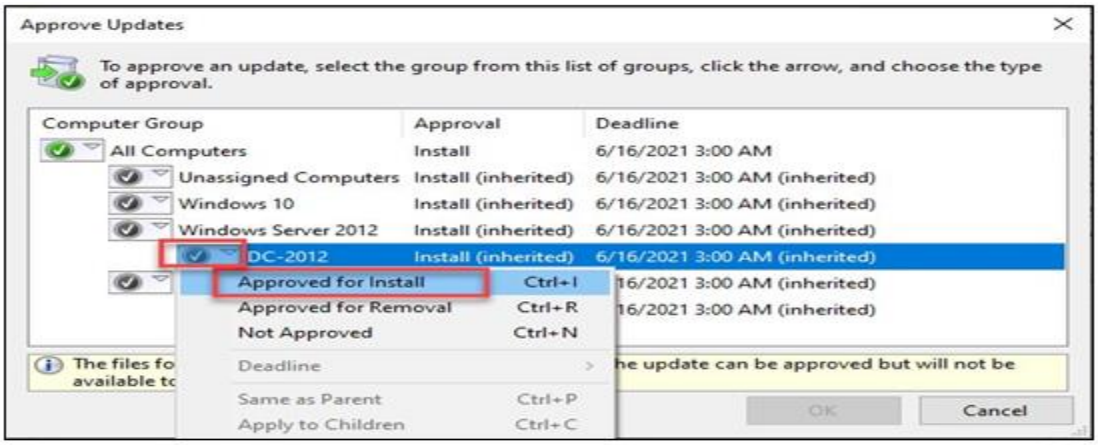
2.3.2. Đối với hệ thống sử dụng WSUS

- 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





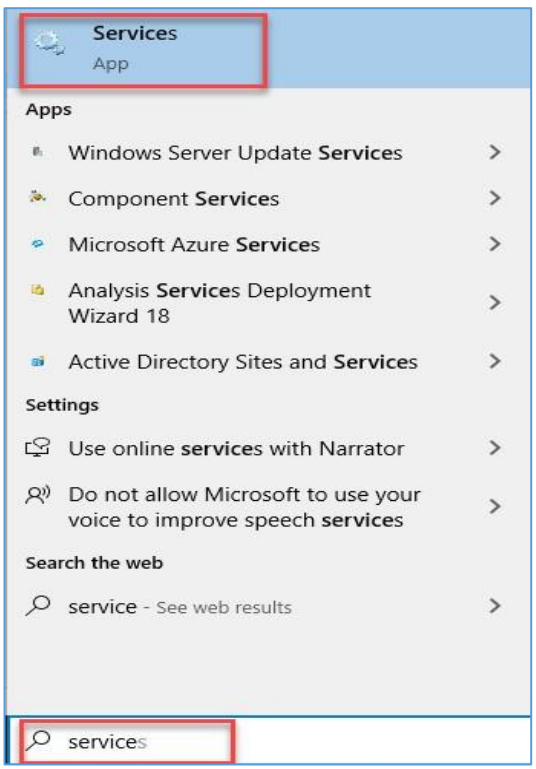
- Bước 3: Cài đặt bản cập nhật và khởi động lại máy chủ.

2.3.3. Kiểm tra lại bản cài đặt trên máy chủ

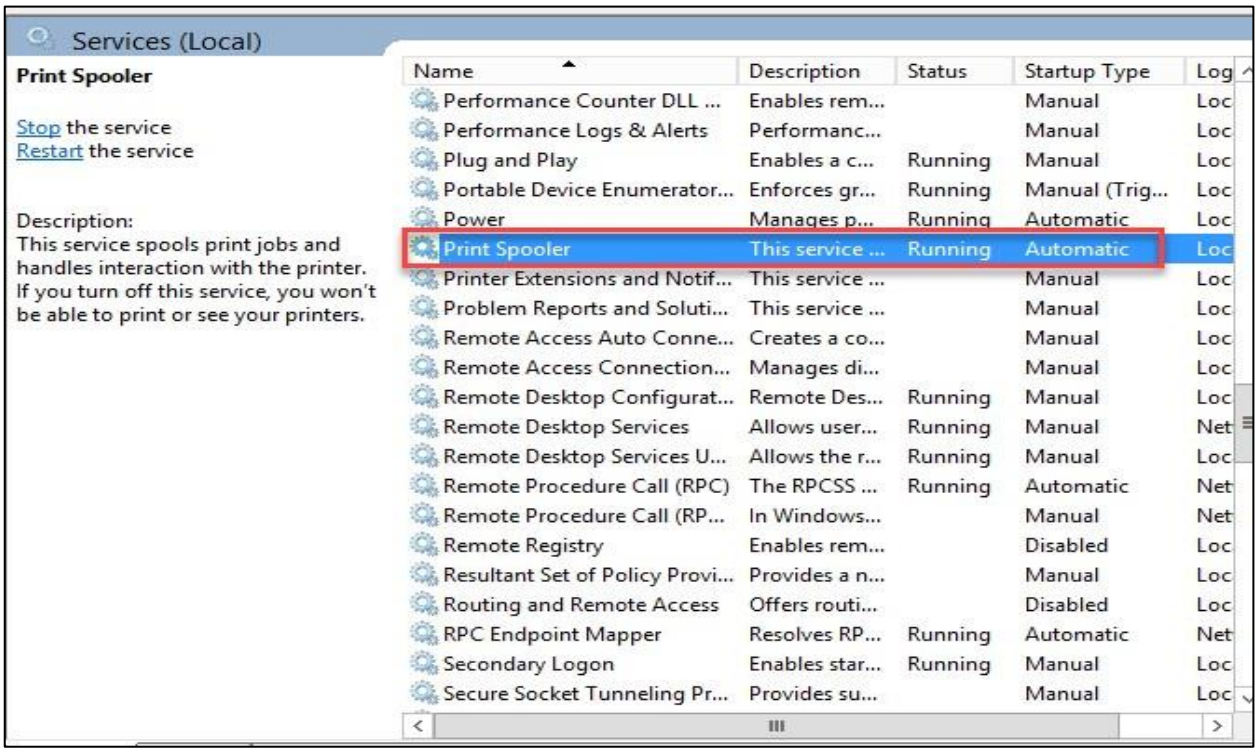
Các bước thực hiện tương tự ở **mục 2.2**.

2.4. Đối với những hệ thống chưa cập nhật được DC (dành cho hệ thống sử dụng WSUS)

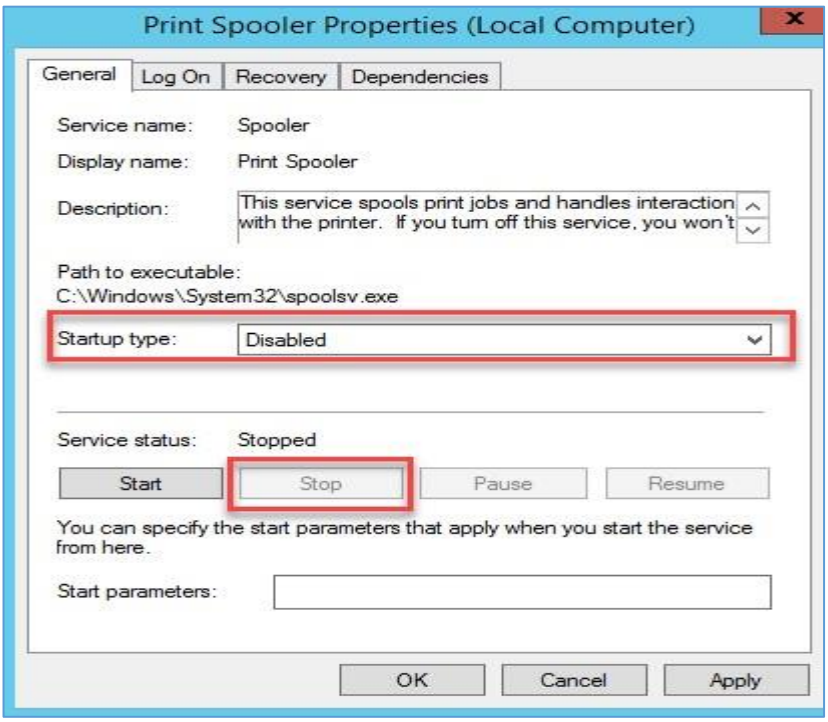
- Bước 1: Vào máy chủ DC, chọn **Start** > Nhập ***services.msc*** > **Enter**



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



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



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

Nguồn tham khảo:

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1675
https://twitter.com/_f0rgetting_/status/1405119285802897410