Dự báo sớm nguy cơ tấn công mạng trên diện rộng

Thực hiện Công văn số 606/STTTT-TTCNTT&TT ngày 30/6/2021 của Sở Thông tin và Truyền thông về việc dự báo sớm nguy cơ tấn công mạng trên diện rộng.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị. Vừa qua, UBND huyện ban hành Công văn về việc dự báo sớm nguy cơ tấn công mạng trên diện rộng. Qua đó giao các cơ quan, đơn vị thực hiện một số nhiệm vụ như sau:

- Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo hướng dẫn của Microsoft.

- Tăng cường giám sát hệ thống thông tin 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.

Chi tiết lỗ hổng và hướng dẫn khắc phục

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/en-US/vulnerability/CVE-2021-1675

2. 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

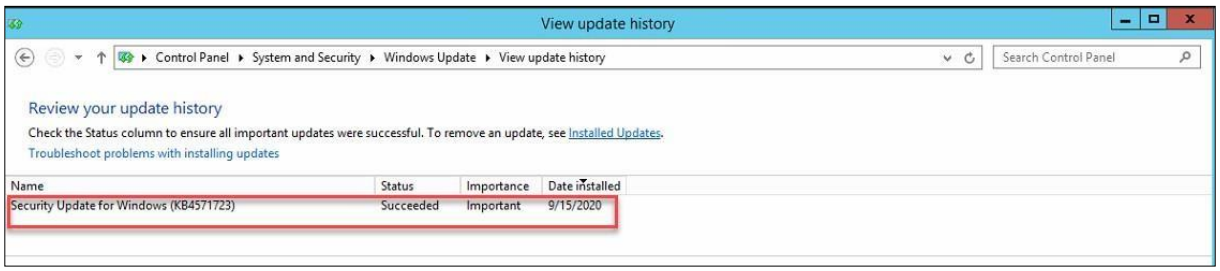
		5003681	Bản update security
23	Windows 8.1 (x64-based Systems)	5003671	Bản update tháng
		5003681	Bản update security
24	Windows RT 8.1	5003671	Bản update tháng

2.2. Hướng dẫn kiểm tra lịch sử cập nhật

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

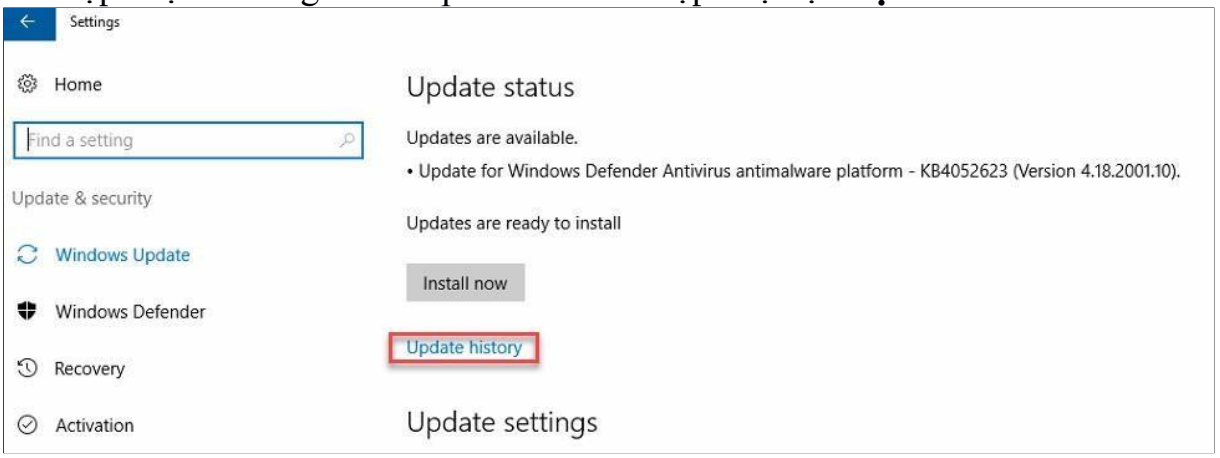
- Windows Server 2012:

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:

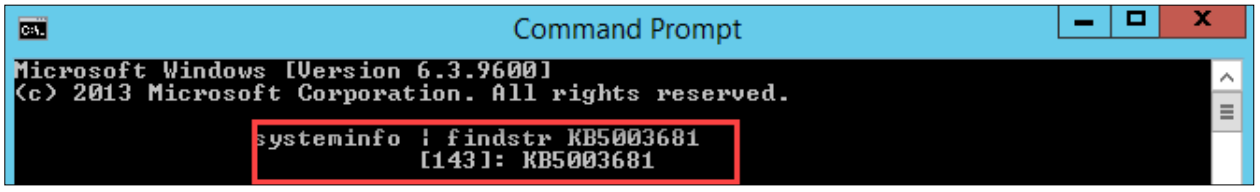
+ Vào thanh công cụ **Start** > **Run** > gõ **cmd.exe** và chọn **OK**

+ 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:



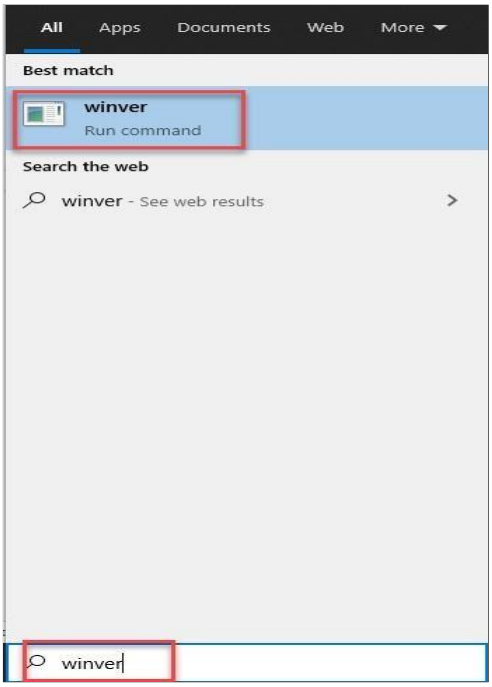
+ Với những máy chủ chưa update, sẽ không hiện ra thông tin:

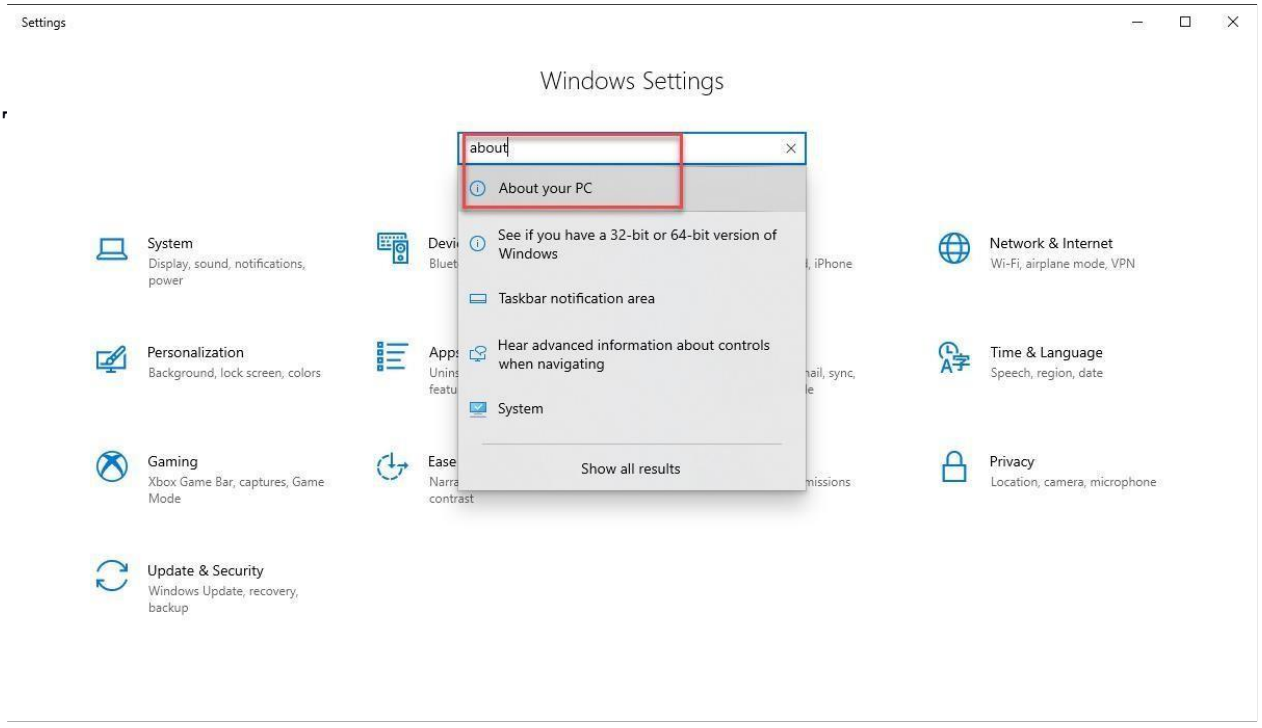
2.3. Hướng dẫn thực hiện cập nhật bản vá

2.3.1. Đối với hệ thống không có máy chủ WSUS

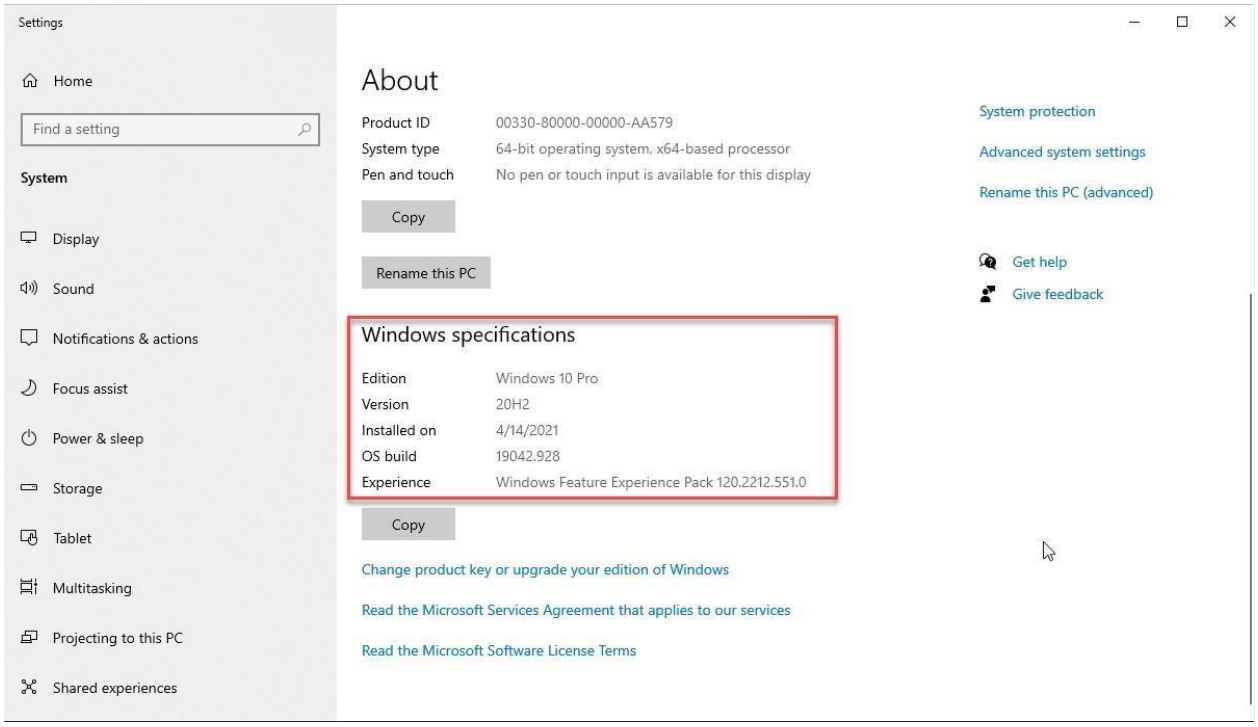
- Bước 1: Kiểm tra OS, version hệ điều hành đang sử dụng:

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



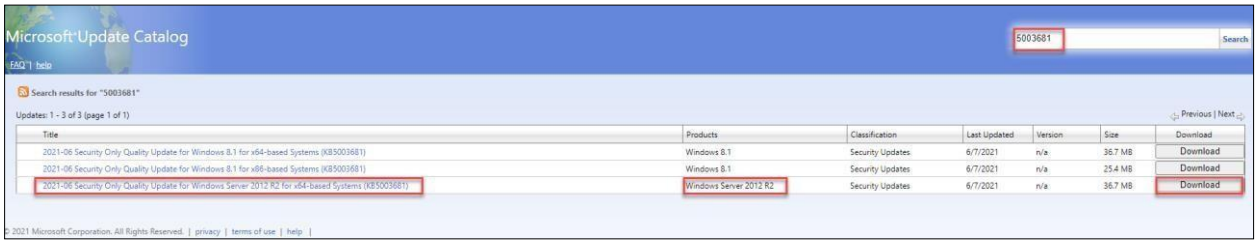


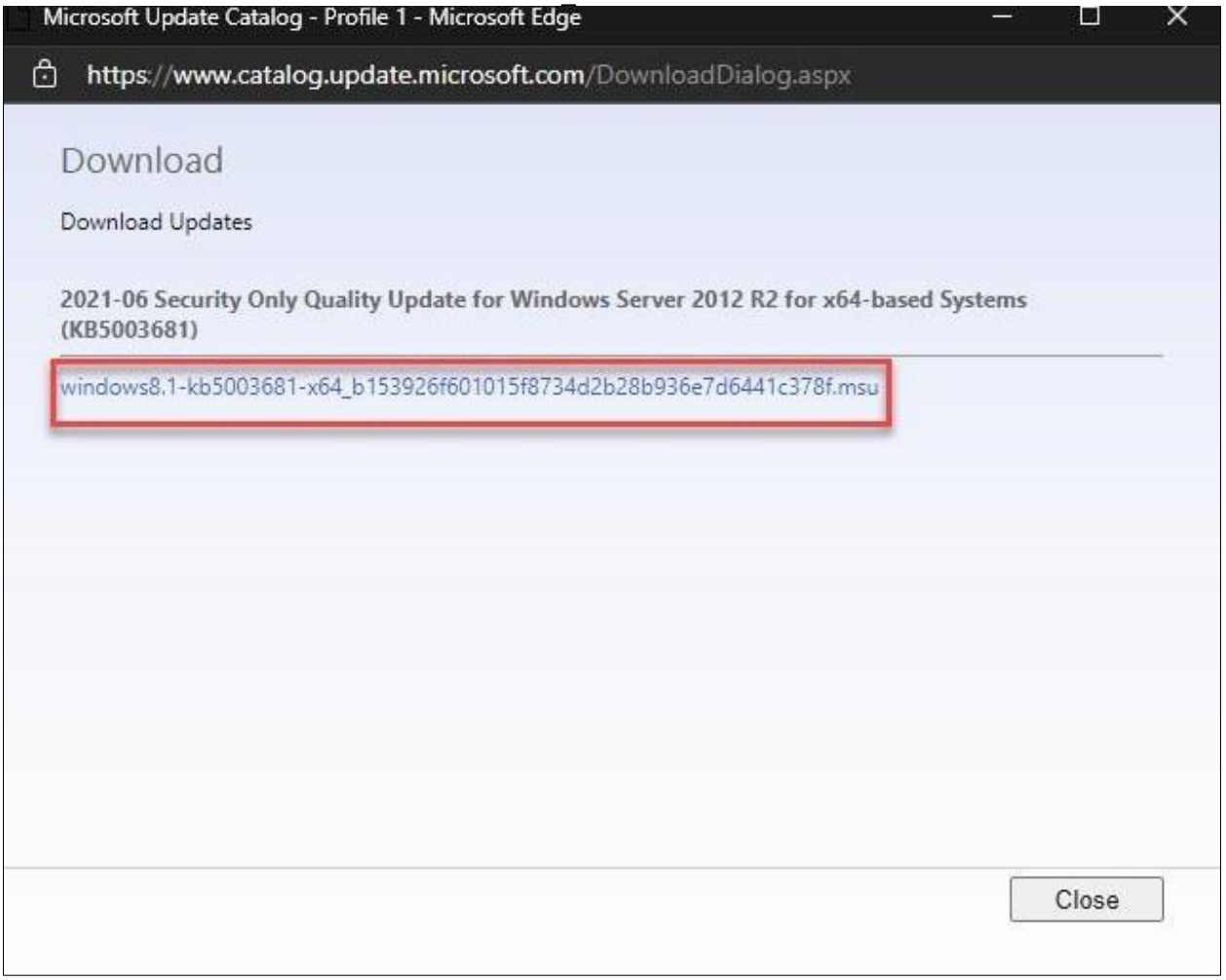
Kiểm tra mục: ***Windows Specifications***



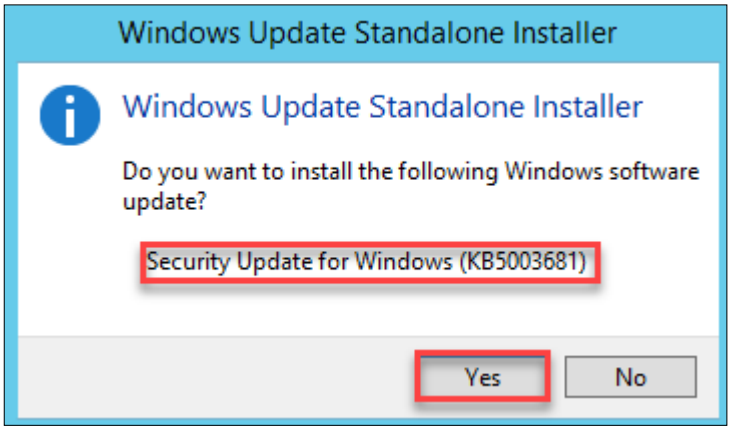
- Bước 2: Download bản vá tại https://www.catalog.update.microsoft.com/Home.aspx

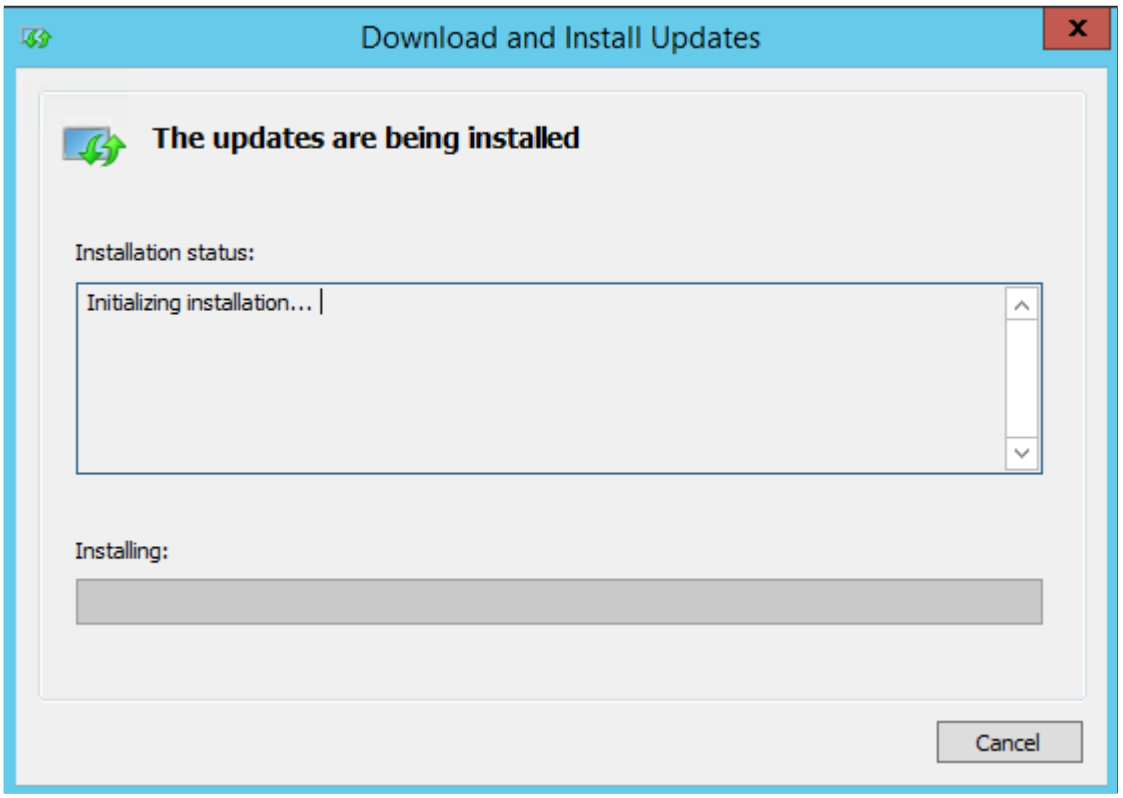
- Bước 3: Tìm và tải bản cập nhật phù hợp cho máy chủ hệ điều hành





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

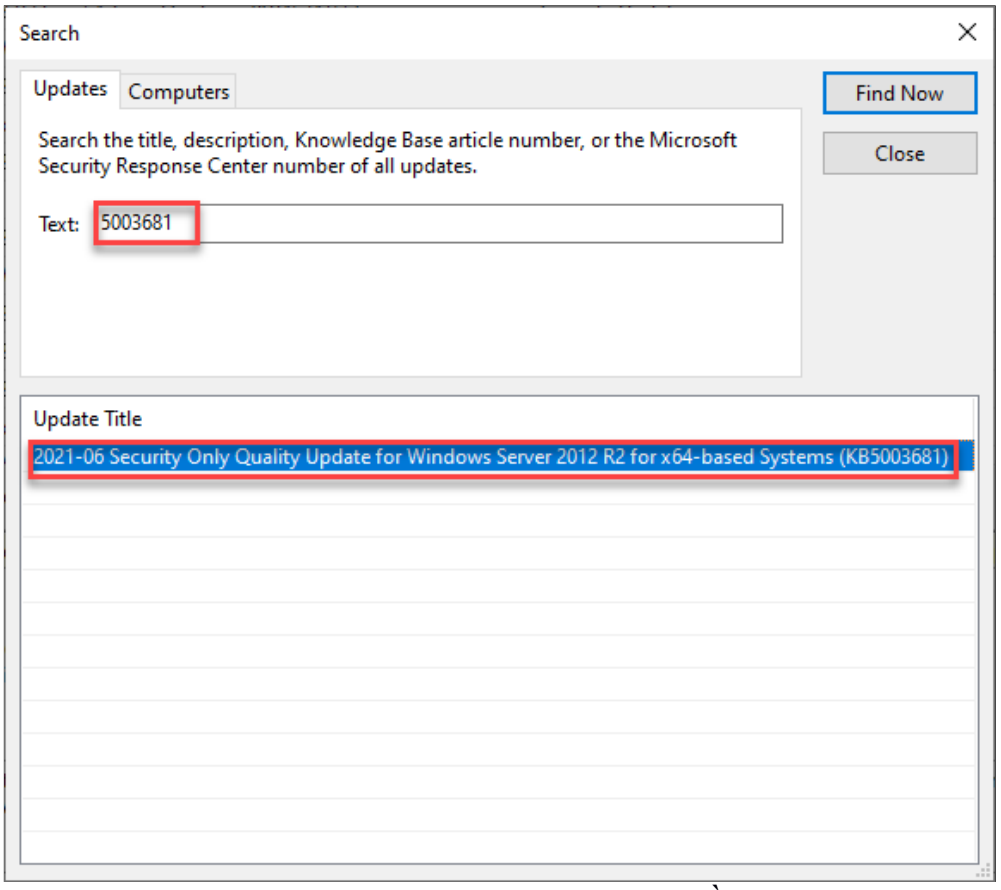




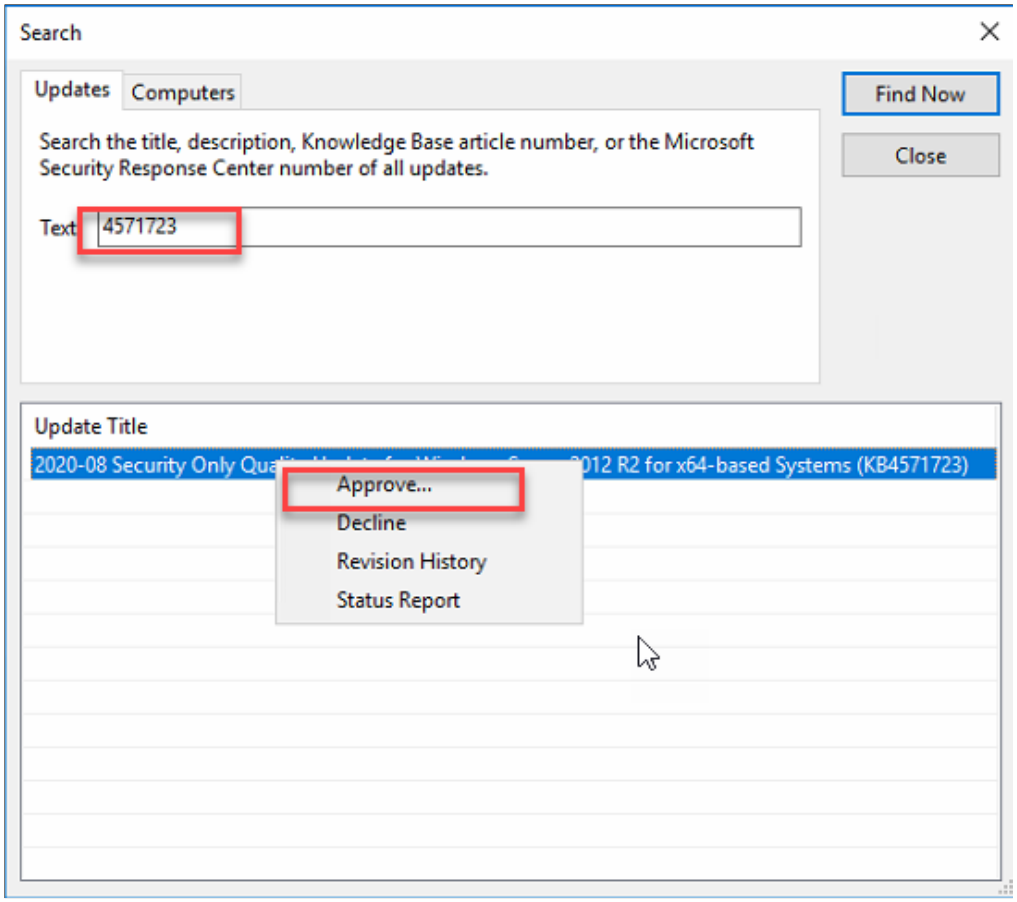
- Bước 5: Khởi động lại máy chủ sau khi tiến hành cài đặt bản cập nhật.

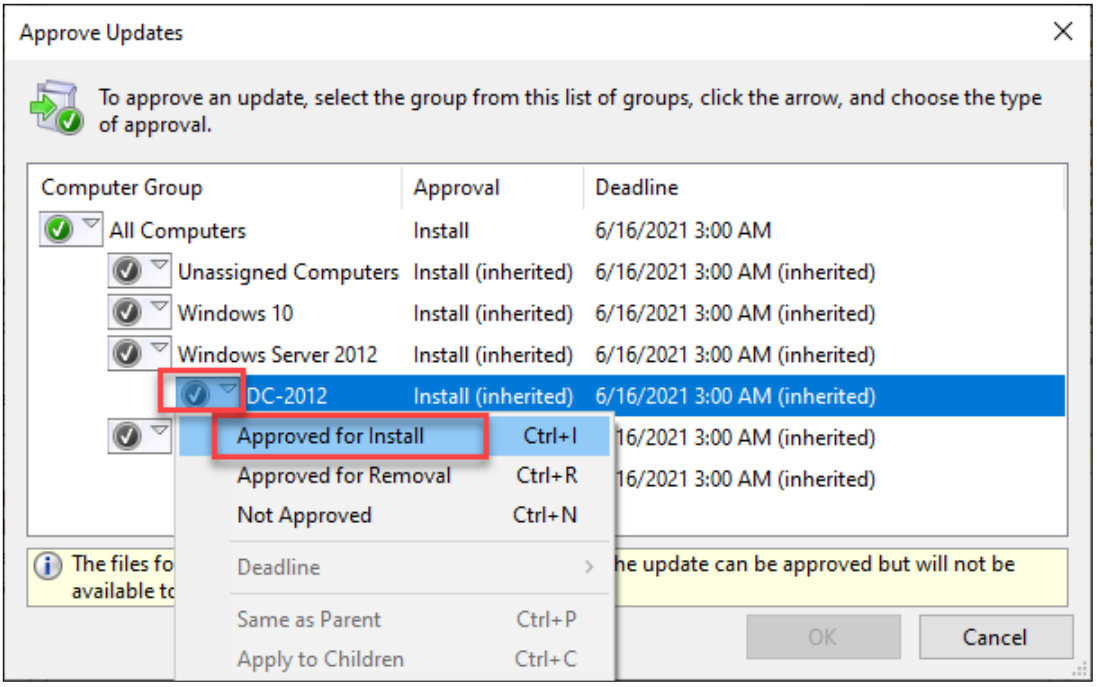
2.3.2. Đối với hệ thống sử dụng WSUS

- Bước 1: Với các hệ thống sử dụng máy chủ WSUS để quản trị các bản cậpnhật 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 bảnupdate





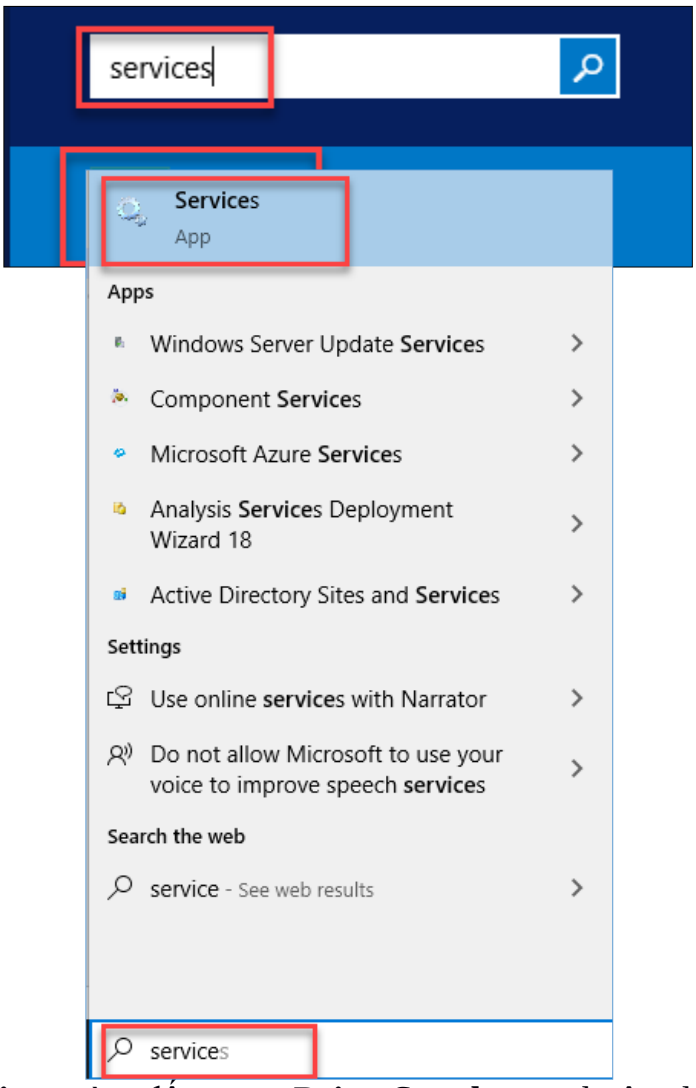
- Bước 3: Cài đặt bản cập nhật và khởi động lại máy chủ.

2.3.3. Kiểm tra lại bản cài đặt trên máy chủ

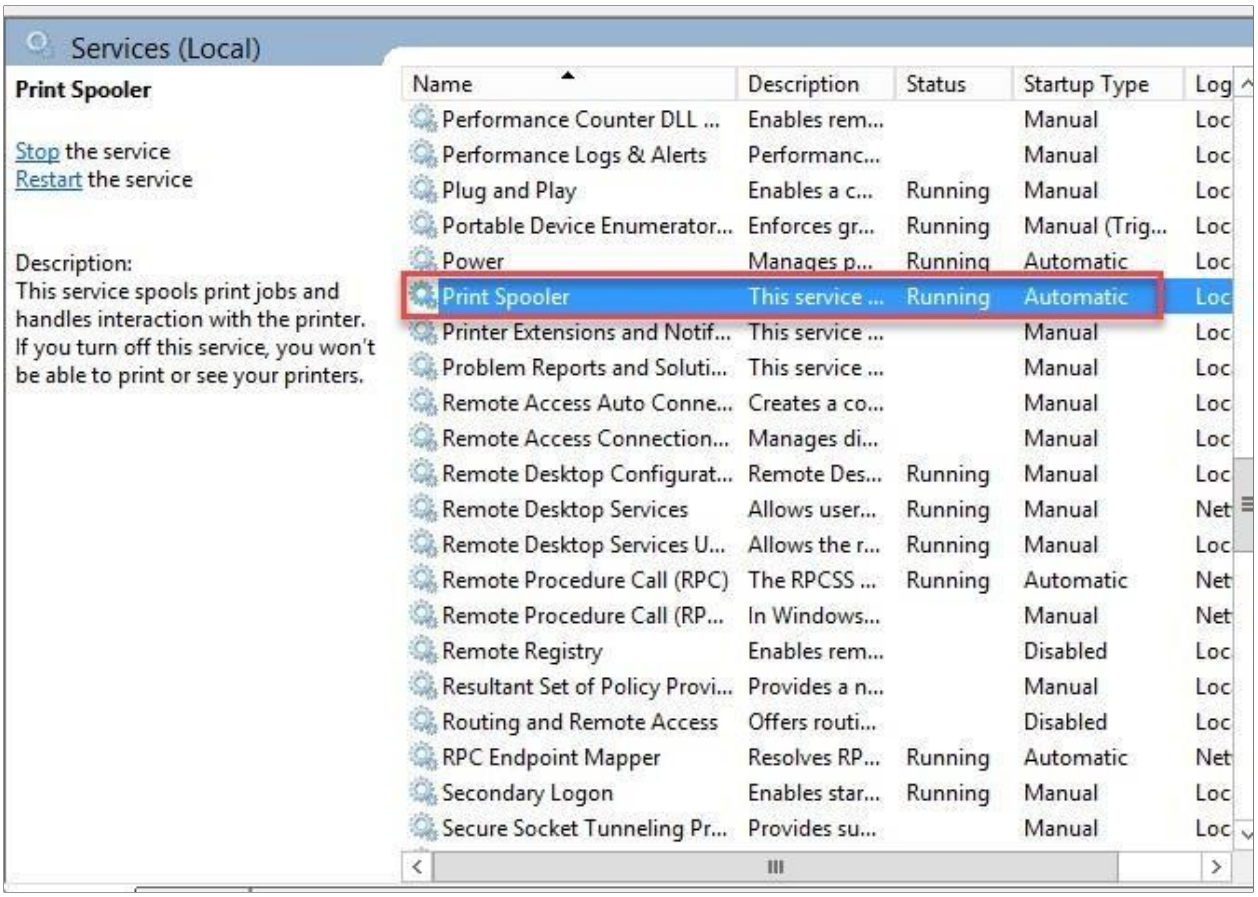
Các bước thực hiện tương tự ở **mục 2.2**.

***2.4.* Đối với những hệ thống chưa cập nhật được DC**

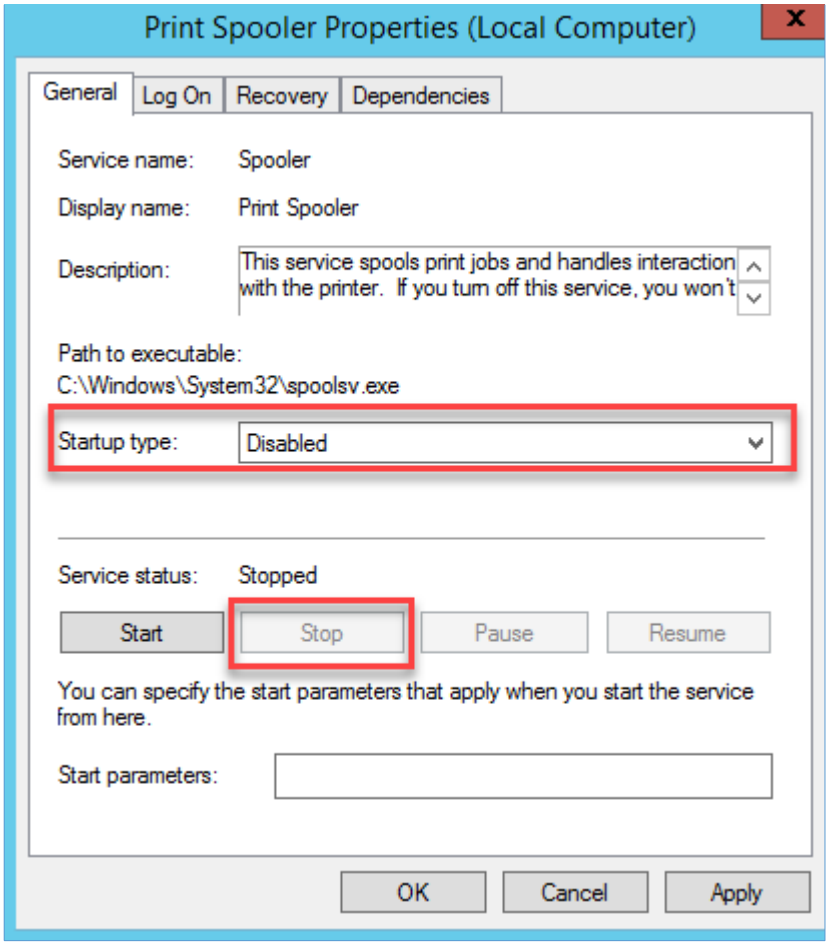
- Bước 1: Vào máy chủ DC, chọn **Start** > Nhập ***services.msc*** > **Enter**



- 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.

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

Văn Vương