VIỆN HÀN LÂM KHOA HỌC VÀ CÔNG NGHỆ VN **TRUNG TÂM TIN HỌC VÀ TÍNH TOÁN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 290 /THTT V/v lỗ hổng bảo mật mới ảnh hưởng đến hệ điều hành Windows 10 và Windows Server	*Hà Nội, ngày 29 tháng 7 năm 2021*

Kính gửi: Các đơn vị trực thuộc
Viện Hàn lâm Khoa học và Công nghệ Việt Nam

Ngày 23/7/2021, Cục An toàn thông tin – Bộ Thông tin và Truyền thông đã ban hành Công văn số 984/CATTT-NCSC thông báo về lỗ hổng bảo mật mới ảnh hưởng đến hệ điều hành Windows 10 và Windows Server. Theo đó, Microsoft đã công bố thông tin về lỗ hổng bảo mật mới (CVE-2021-36934) ảnh hưởng đến hệ điều hành Windows 10 phiên bản 1809/1909/2004/21H1/20H2, Windows Server 2019/20H2 vào ngày 20/7/2021. Lỗ hổng này nếu khai thác được sẽ cho phép đối tượng tấn công nâng cao đặc quyền trên hệ thống mục tiêu, từ đó có thể chiếm quyền điều khiển toàn bộ hệ thống.

Theo đánh giá sơ bộ của Trung tâm Giám sát an toàn không gian mạng Quốc gia (NCSC), hệ điều hành Windows 10 và Windows Server được sử dụng khá phổ biến hiện nay nên lỗ hổng bảo mật này sẽ có ảnh hưởng tương đối rộng và có thể trở thành mục tiêu hướng đến của các đối tượng tấn công trong thời gian tới. Đặc biệt tại thời điểm này, lỗ hổng bảo mật chưa có bản vá đồng thời lại có mã khai thác công khai trên Internet. Do vậy, việc khai thác lỗ hổng trở nên dễ dàng hơn dẫn đến gia tăng các nguy cơ tấn công mạng.

Thực hiện chỉ đạo của Lãnh đạo Viện Hàn lâm nhằm đảm bảo an toàn cho hệ thống thông tin của các đơn vị trực thuộc và góp phần bảo đảm an toàn cho không gian mạng tại Viện Hàn lâm, Trung tâm Tin học và Tính toán khuyến nghị Quý đơn vị thực hiện một số giải pháp sau:

1. Kiểm tra, rà soát và xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Người sử dụng có thể thực hiện biện pháp khắc phục thay thế để giảm thiểu nguy cơ tấn công theo hướng dẫn của Microsoft *(chi tiết tham khảo tại Phụ lục kèm theo).*

2. 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.

Quá trình thực hiện nếu phát sinh vướng mắc, đề nghị liên hệ với Phòng Đảm bảo công nghệ thông tin - Trung tâm Tin học và Tính toán (điện thoại: 024.37914773, thư điện tử: *sinhtv@cic.vast.vn*) để được hỗ trợ.

Trân trọng ./.

Nơi nhận:
- Như trên;
- Viện Hàn lâm KHCNVN (để b/c);
- PCT. Trần Tuấn Anh (để b/c);
- Giám đốc (để b/c);
- Lưu: VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

VIỆN HÀN LÂM KHOA HỌC VÀ CÔNG NGHỆ VIỆT NAM
TRUNG TÂM TIN HỌC VÀ TÍNH TOÁN

Ngô Văn Thanh

PHỤ LỤC
Thông tin về lỗ hổng bảo mật
(Kèm theo Công văn số /THTT ngày /7/2021 của Trung tâm Tin học và Tính toán)

1. Thông tin về các lỗ hổng

Mã lỗ hổng: CVE-2021-36934

CVSS: 7.8 (cao)

Mô tả: Lổ hổng bảo mật tồn tại do các tài khoản người dùng thường có thể truy cập vào các tệp hệ thống (như các tệp SAM, Windows Registry). Khai thác thành công lỗ hổng này, cho phép đối tượng tấn công thực thi mã tùy ý với đặc quyền cao hơn trên hệ thống mục tiêu.

Sản phẩm bị ảnh hưởng: Cho đến thời điểm này theo công bố của Microsoft xác nhận rằng lỗ hổng này ảnh hưởng đến hệ điều hành Windows 10 phiên bản 1809/1909/2004/21H1/20H2, Windows Server 2019/20H2.

2. Hướng dẫn khắc phục

Hiện tại, Microsoft chưa có thông tin phát hành bản vá cho lỗ hổng này, thay vào đó là đưa ra biện pháp khắc phục thay thế để giảm thiểu nguy cơ.

2.1. Danh sách các phiên bản hệ điều hành bị ảnh hưởng

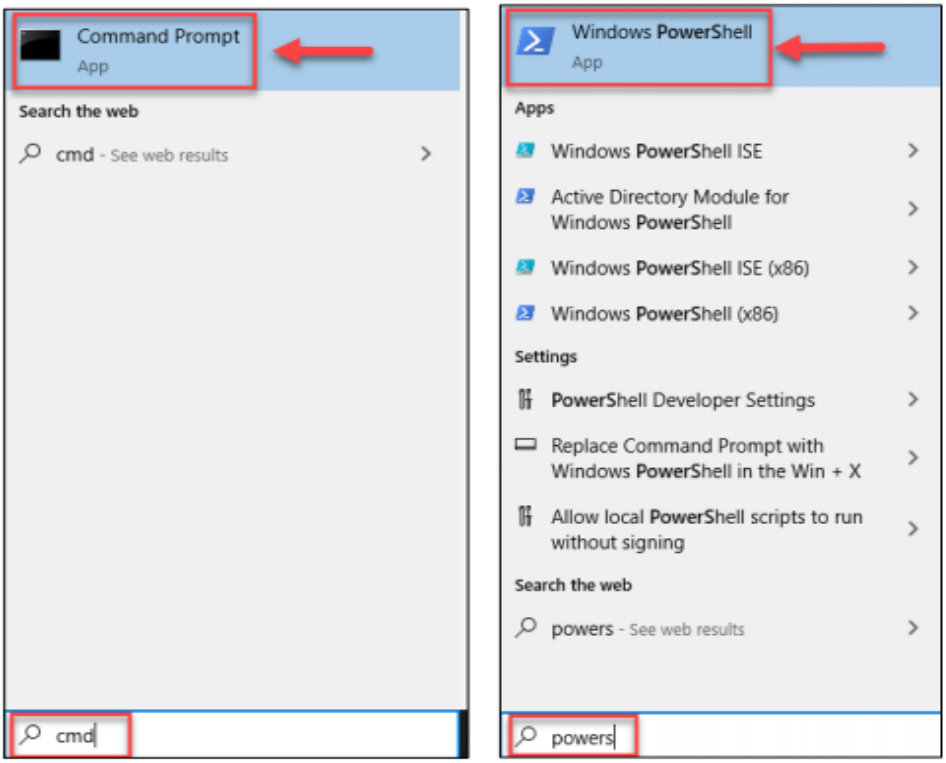
STT	Hệ điều hành
1	Windows Server, version 20H2 (Server Core Installation)
2	Windows 10 Version 20H2 ARM64-based Systems
3	Windows 10 Version 20H2 for 32-bit System
4	Windows 10 Version 20H2 for x64-based Systems
5	Windows Server, version 2004 (Server Core Installation)
6	Windows 10 Version 2004 for x64-based Systems
7	Windows 10 Version 2004 for ARM64-based Systems
8	Windows 10 Version 2004 for 32-bit Systems
9	Windows 10 Version 21H1 for 32-bit Systems
10	Windows 10 Version 21H1 for ARM64-based Systems
11	Windows 10 Version 21H1 for x64-based Systems
12	Windows 10 Version 1909 for ARM64-based Systems
13	Windows 10 Version 1909 for x64-based Systems
14	Windows 10 Version 1909 for 32-bit Systems
15	Windows Server 2019 (Server Core installation)
16	Windows Server 2019
17	Windows 10 Version 1809 for ARM64-based Systems
18	Windows 10 Version 1809 for x64-based Systems
19	Windows 10 Version 1809 for 32-bit Systems

2.2. Hướng dẫn các bước khắc phục

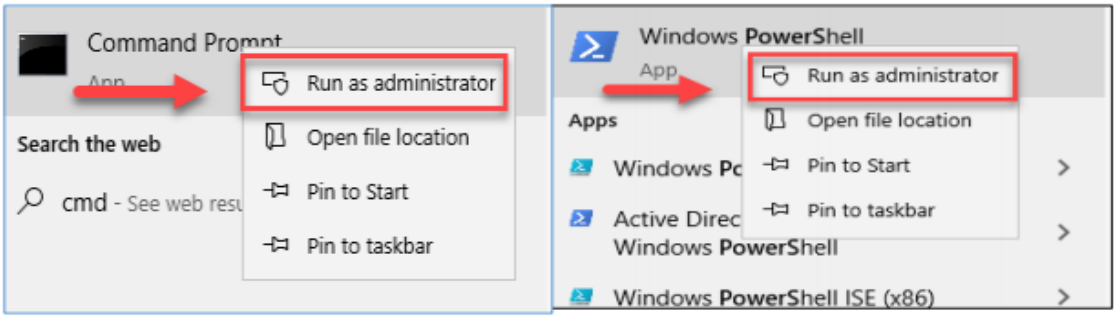
- Bước 1: Đối với các máy tính sử dụng hệ điều hành trong danh sách tại **mục 2.1**

+ Mở **Command Prompt** hoặc **Windows PowerShell** bằng quyền **Admin**

+ Trên thanh **Start** > nhập **cmd** hoặc **powershel**



+ Nháy phải chuột, chọn **Run as administrator** > chọn **YES** khi có bảng thông báo hiện ra



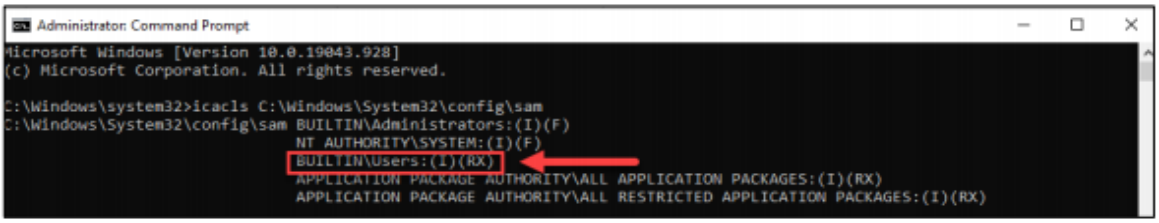
+ Kiểm tra máy tính có bị ảnh hưởng lỗ hổng **CVE-2021-36934**, trên **Command Prompt** hoặc **Windows PowerShell**, sử dụng lệnh:

icacls C:\Windows\System32\config\sam

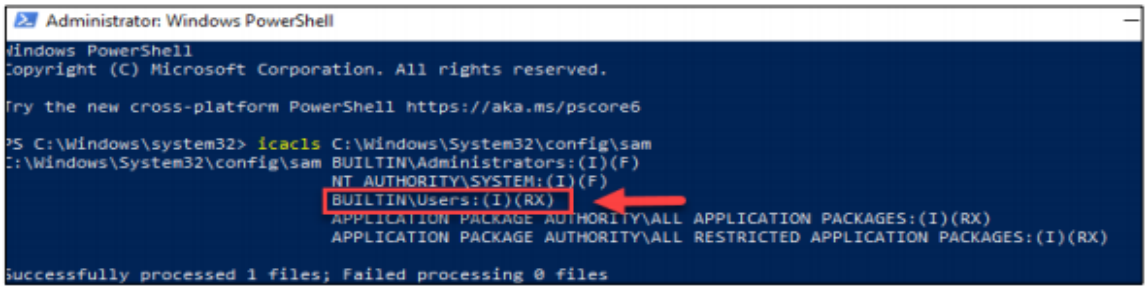
+ Nếu hiển thị **BUILTIN\Users:(I)(RX)**, máy tính bị ảnh hưởng bởi lỗ hổng. Thực hiện tiếp các bước sau để khắc phục lỗ hổng.

+ Nếu không hiển thị lỗi như hình dưới đây, máy tính không bị ảnh hưởng và không cần thực hiện các bước tiếp theo.

+ Trên giao diện **Command Prompt**



+ Trên giao diện **Windows PowerShell**

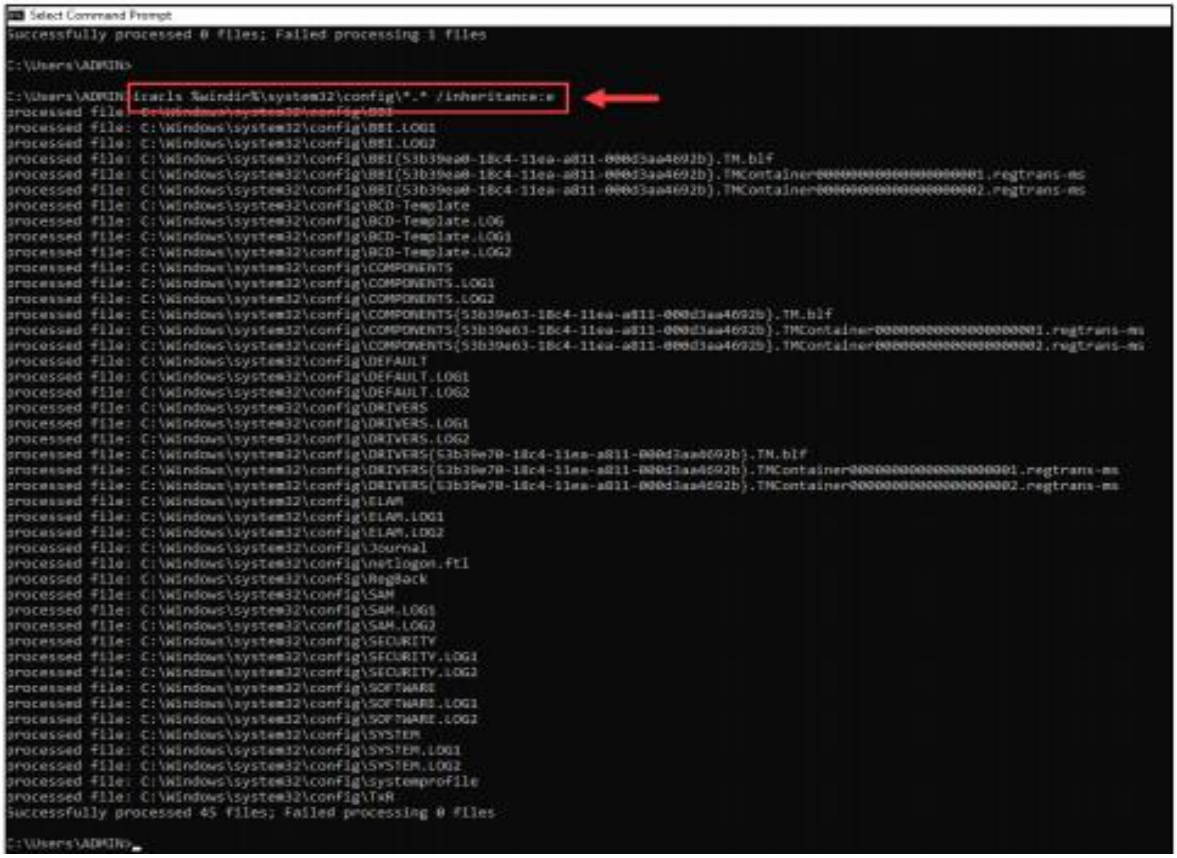


Nếu kết quả nhận được giống như thông tin theo ảnh ở trên thì máy tính đang bị ảnh hưởng bởi lỗ hổng CVE-2021-36934, Quý đơn vị tiến hành khắc phục tạm thời theo hướng dẫn các bước tiếp theo.

- **Bước 2:** Sử dụng lệnh để hạn chế quyền truy cập vào thư mục **%windir%\system32\config**

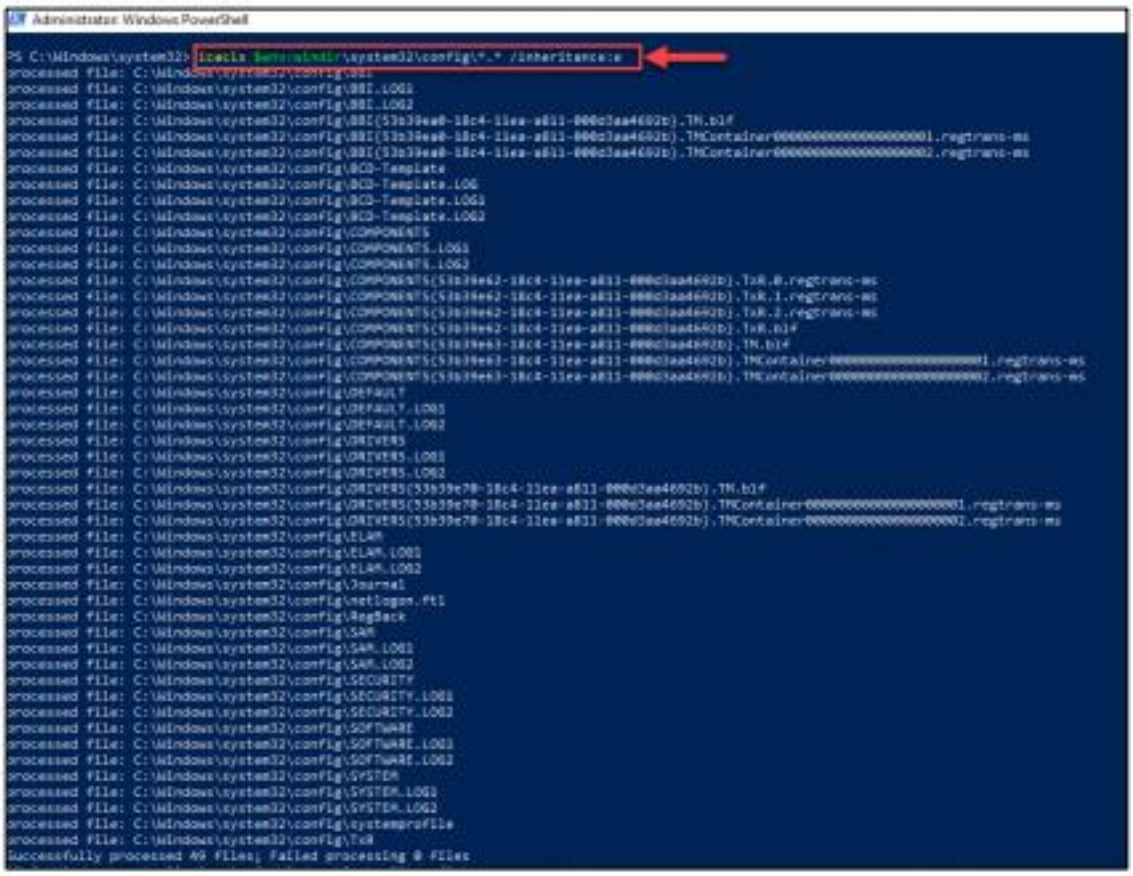
+ Trên giao diện **Command Prompt** sử dụng lệnh:

icacls %windir%\system32\config.* /inheritance:e*



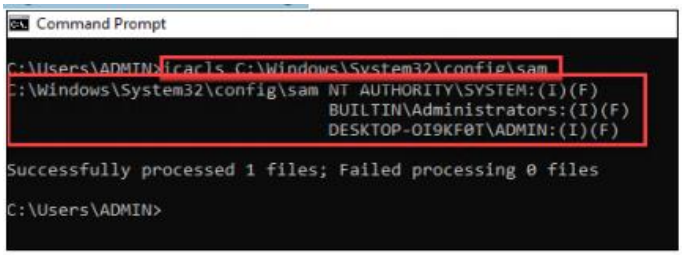
+ Trên giao diện **Windows PowerShell** sử dụng lệnh:

icacls $env:windir\system32\config.* /inheritance:e*

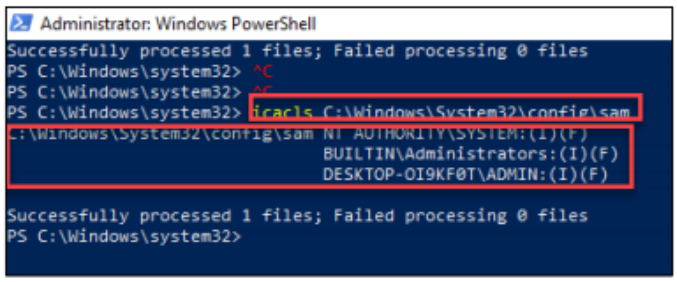


- **Bước 3**: Kiểm tra lại quyền thư mục như ở **Bước 1:**

+ Trên giao diện **Command Prompt**



+ Trên giao diện **Windows PowerShell**



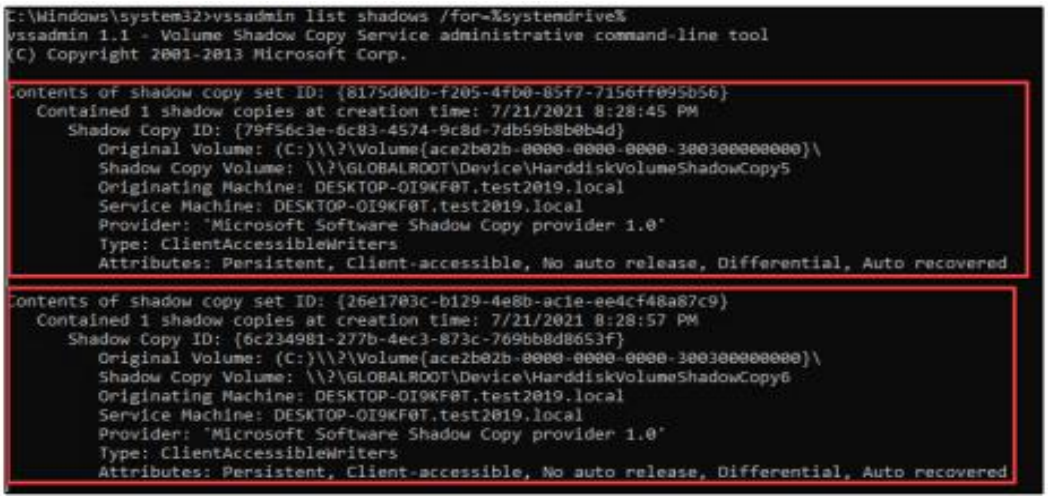
- **Bước 4:** Xóa các bản sao của **Volume Shadow Copy Service, System Restore** (nếu có)

Lưu ý: *Việc thực hiện xóa **Shadow Copy** có thể ảnh hưởng đến hoạt động khôi phục, bao gồm khả năng khôi phục dữ liệu bằng các ứng dụng sao lưu của bên thứ ba.*

+ **Cách 1:** Sử dụng lệnh trên **Command Prompt**

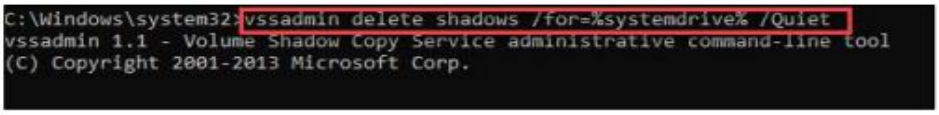
** Hiển thị tất cả các bản sao lưu* ***Shadow Copy:***

vssadmin list shadows /for=%systemdrive%



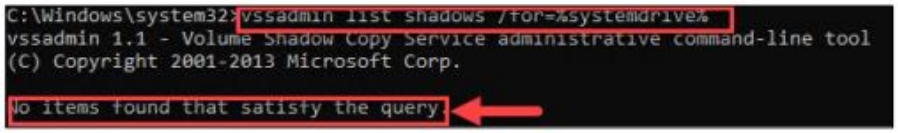
** Xoá toàn bộ các bản sao lưu:*

vssadmin delete shadows /for=%systemdrive% /Quiet



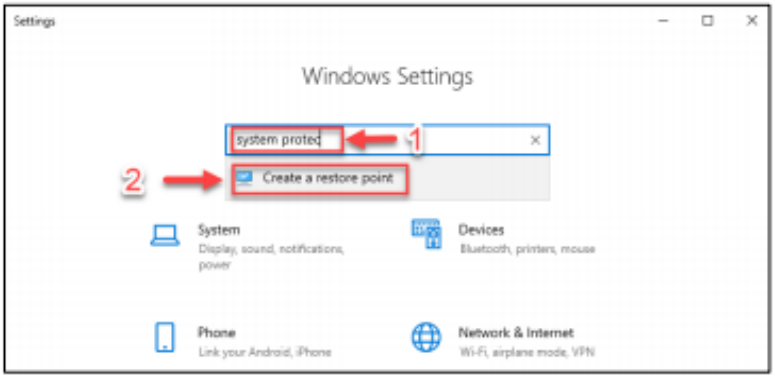
** Kiểm tra lại các bản sao lưu đã bị xóa hay chưa:*

vssadmin list shadows /for=%systemdrive%

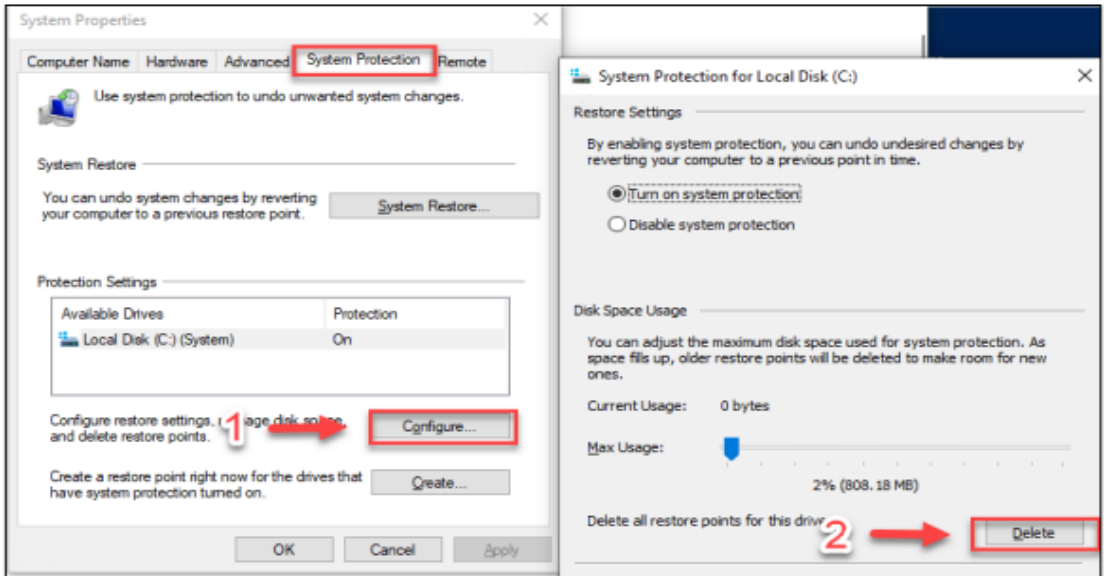


+ **Cách 2:** Sử dụng giao diện

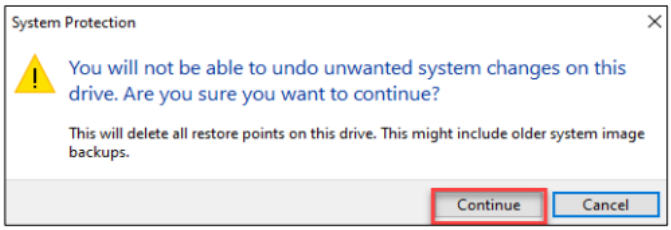
* Truy cập **Settings** > nhập vào ô tìm kiếm **System protect** > Chọn mục **Create a restore point**



***** Tại tab **System Protection** > Chọn **Configure** > chọn **Delete** tại **Detele all restore points for this drive** trên cửa sổ pop-up mới hiện lên

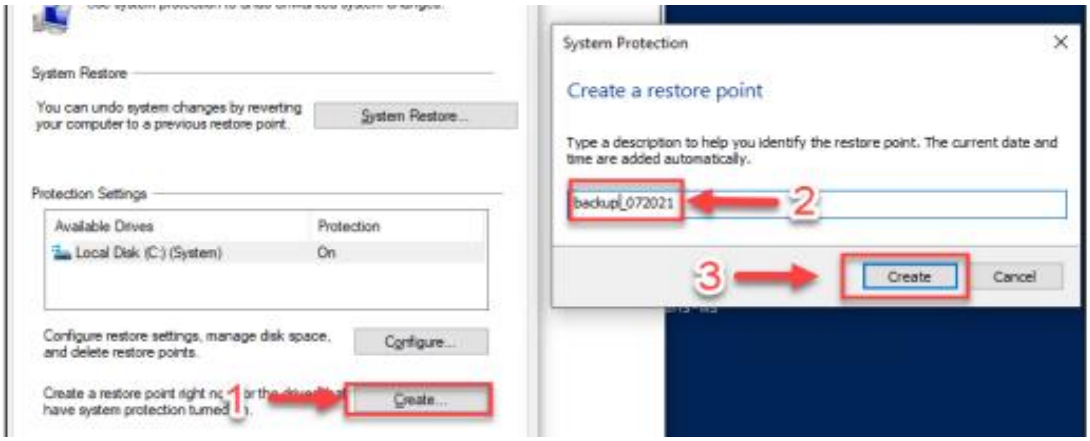


* Chọn **Continue** để hoàn tất việc xóa các bản sao



* Kiểm tra các bản sao lưu đã được xóa: Tại tab **System Protection** > Chọn **System Restore**

* Tạo bản sao lưu mới (nếu cần): Tại tab **System Protection** > Chọn **Create**



Nguồn tham khảo:

- Công văn số 984/CATTT-NCSC ngày 23/7/2021 của Cục An toàn thông tin – Bộ Thông tin và Truyền thông;

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934