

Số: /TTCNTT-KTHT
V/v lỗ hổng bảo mật mới ảnh hưởng đến hệ
điều hành Windows 10 và Windows Server

Hà Nội, ngày tháng năm 2021

Kính gửi: Các đơn vị trực thuộc Bộ

Theo Công văn số 984/CATTT-NCSC ngày 23/7/2021 của Cục An toàn thông tin về việc lỗ hổng bảo mật mới ảnh hưởng đến hệ điều hành Windows 10 và Windows Server, ngày 20/7/2021, 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. Khai thác thành công lỗ hổng này 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 Cục An toàn thông tin – Bộ Thông tin và Truyền thông, 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.

Nhằm bảo đảm an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát và xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Tại thời điểm này chưa có bản vá bảo mật cho các máy bị ảnh hưởng, Quý đơn vị cần 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.

Trong trường hợp cần thiết, Quý đơn vị liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongkttht@most.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Công thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

Hà Quốc Trung

Phụ lục
Thông tin về lỗ hổng bảo mật
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021 của Trung tâm
Công nghệ thông tin)

1. Thông tin về các lỗ hổng

Mã lỗ hổng: CVE-2021-36934

CVSS: 7.8 (cao)

Mô tả: Lỗ 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 bị tấn công.

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)

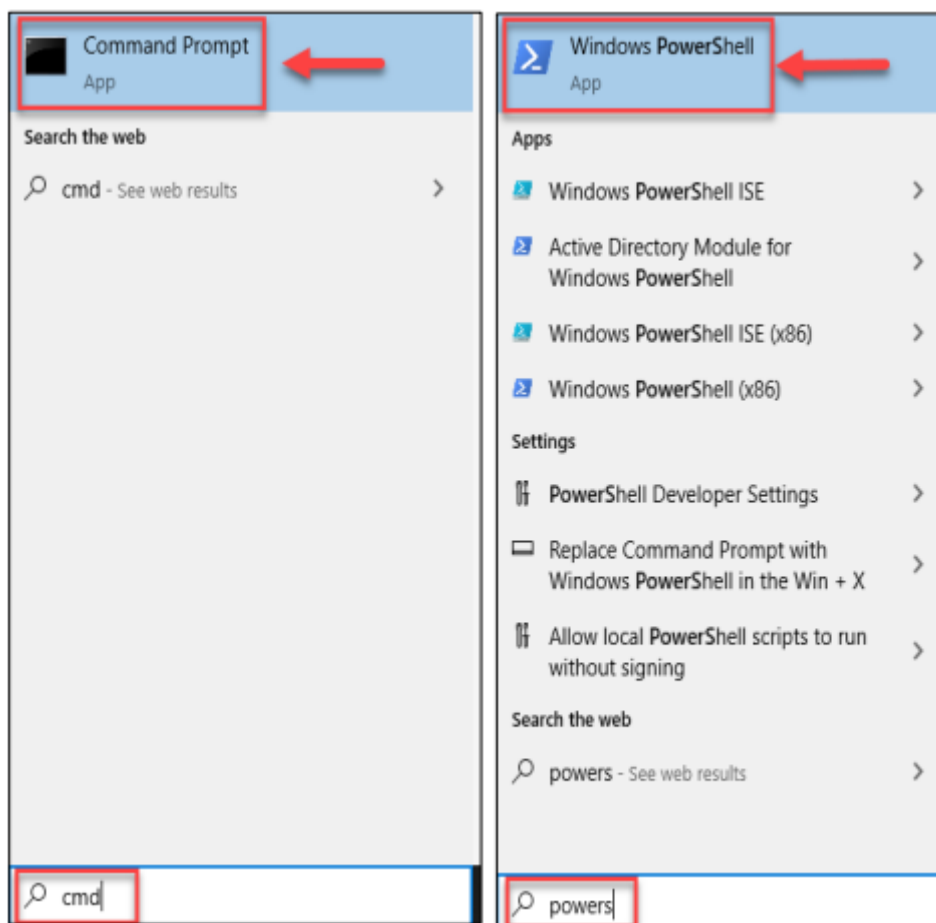
16	Windows Server 2019
17	Windows 10 Version 1809 for ARM64-based Systems
18	Windows 10 Version 1809 for x64-based Systems
19	Windows 10 Version 1809 for 32-bit Systems

2.2. Hướng dẫn các bước khắc phục

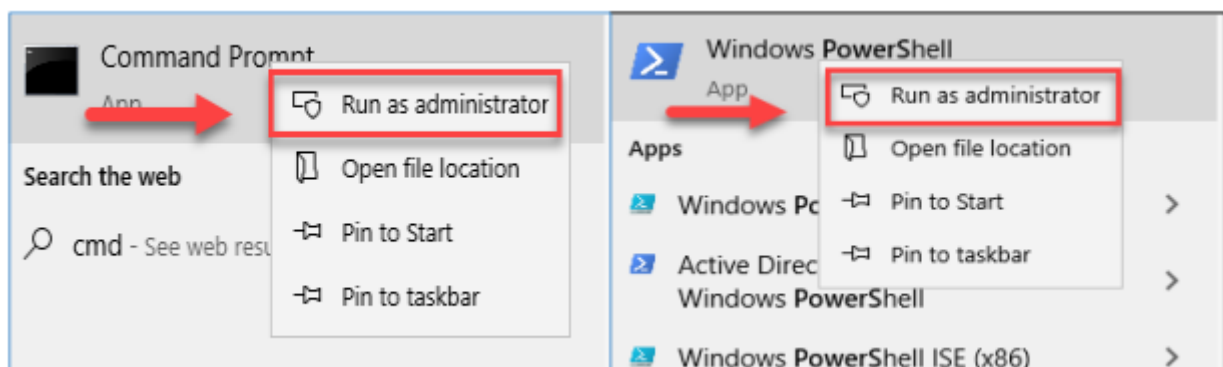
- **Bước 1:** Đối với các máy tính sử dụng hệ điều hành trong danh sách tại **mục 2.1**

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

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



+ Chuột phải 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:

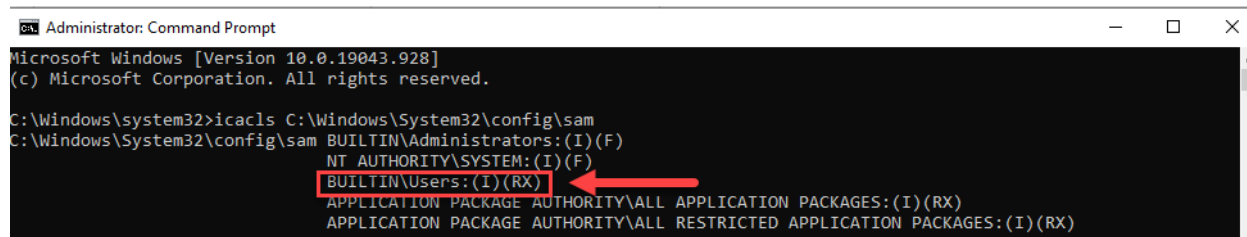
```
icacls C:\Windows\System32\config\sam
```

+ 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.

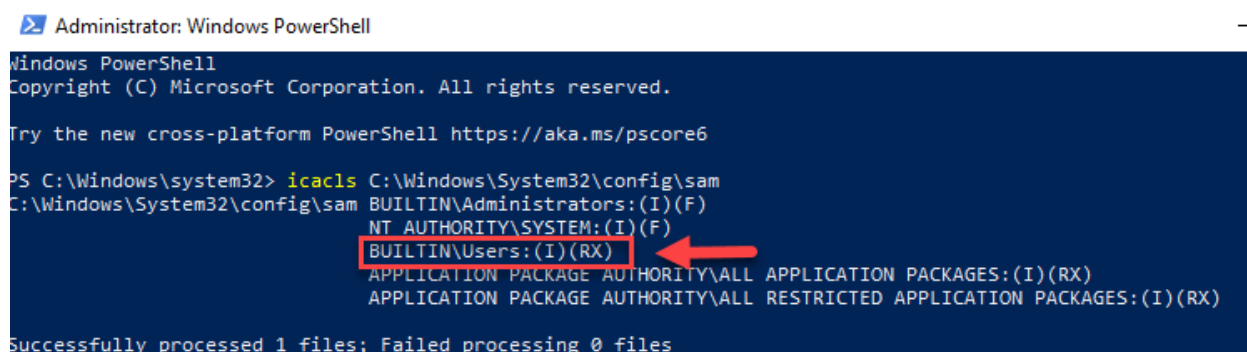
*** Trên giao diện Command Prompt:**



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>icacls C:\Windows\System32\config\sam
C:\Windows\System32\config\sam BUILTIN\Administrators:(I)(F)
NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Users:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
```

*** Trên giao diện Windows PowerShell**



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> icacls C:\Windows\System32\config\sam
C:\Windows\System32\config\sam BUILTIN\Administrators:(I)(F)
NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Users:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)

Successfully processed 1 files; Failed processing 0 files
```

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
```


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

+ *Trên giao diện Command Prompt*

```
Command Prompt
C:\Users\ADMIN>icacls C:\Windows\System32\config\sam
C:\Windows\System32\config\sam NT AUTHORITY\SYSTEM:(I)(F)
                        BUILTIN\Administrators:(I)(F)
                        DESKTOP-OI9KF0T\ADMIN:(I)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\ADMIN>
```

+ *Trên giao diện Windows PowerShell*

```
Administrator: Windows PowerShell
Successfully processed 1 files; Failed processing 0 files
PS C:\Windows\system32> ^C
PS C:\Windows\system32> ^C
PS C:\Windows\system32> icacls C:\Windows\System32\config\sam
C:\Windows\System32\config\sam NT AUTHORITY\SYSTEM:(I)(F)
                        BUILTIN\Administrators:(I)(F)
                        DESKTOP-OI9KF0T\ADMIN:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\Windows\system32>
```

- **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%
```

```
C:\Windows\system32>vssadmin list shadows /for=%systemdrive%
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {8175d0db-f205-4fb0-85f7-7156ff095b56}
  Contained 1 shadow copies at creation time: 7/21/2021 8:28:45 PM
    Shadow Copy ID: {79f56c3e-6c83-4574-9c8d-7db59b8b0b4d}
    Original Volume: (C:)\?\Volume{ace2b02b-0000-0000-0000-300300000000}\
    Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy5
    Originating Machine: DESKTOP-OI9KF0T.test2019.local
    Service Machine: DESKTOP-OI9KF0T.test2019.local
    Provider: 'Microsoft Software Shadow Copy provider 1.0'
    Type: ClientAccessibleWriters
    Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered

Contents of shadow copy set ID: {26e1703c-b129-4e8b-ac1e-ee4cf48a87c9}
  Contained 1 shadow copies at creation time: 7/21/2021 8:28:57 PM
    Shadow Copy ID: {6c234981-277b-4ec3-873c-769bb8d8653f}
    Original Volume: (C:)\?\Volume{ace2b02b-0000-0000-0000-300300000000}\
    Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6
    Originating Machine: DESKTOP-OI9KF0T.test2019.local
    Service Machine: DESKTOP-OI9KF0T.test2019.local
    Provider: 'Microsoft Software Shadow Copy provider 1.0'
    Type: ClientAccessibleWriters
    Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered
```

*** Xóa toàn bộ các bản sao lưu:**

```
vssadmin delete shadows /for=%systemdrive% /Quiet
```

```
C:\Windows\system32>vssadmin delete shadows /for=%systemdrive% /Quiet
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.
```

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

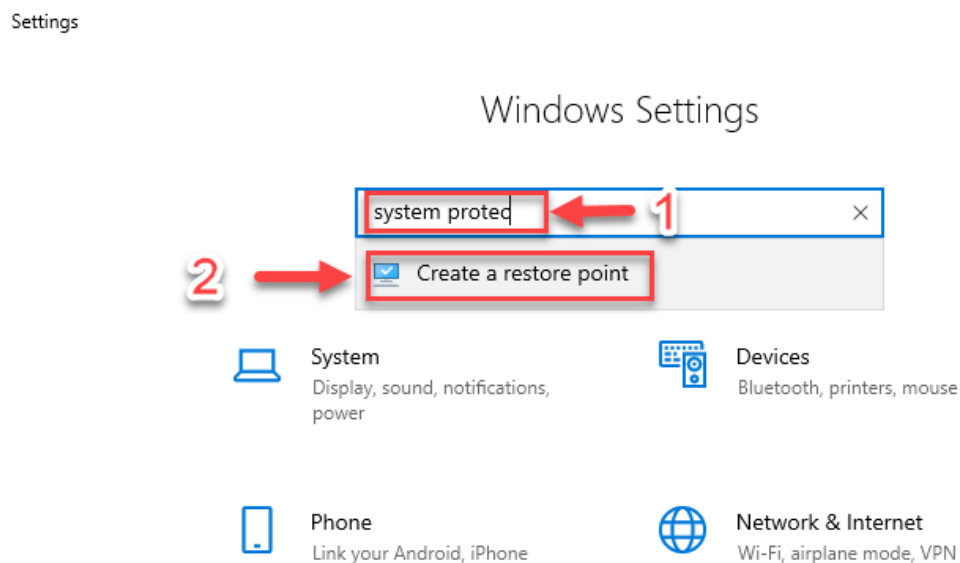
```
vssadmin list shadows /for=%systemdrive%
```

```
C:\Windows\system32>vssadmin list shadows /for=%systemdrive%
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

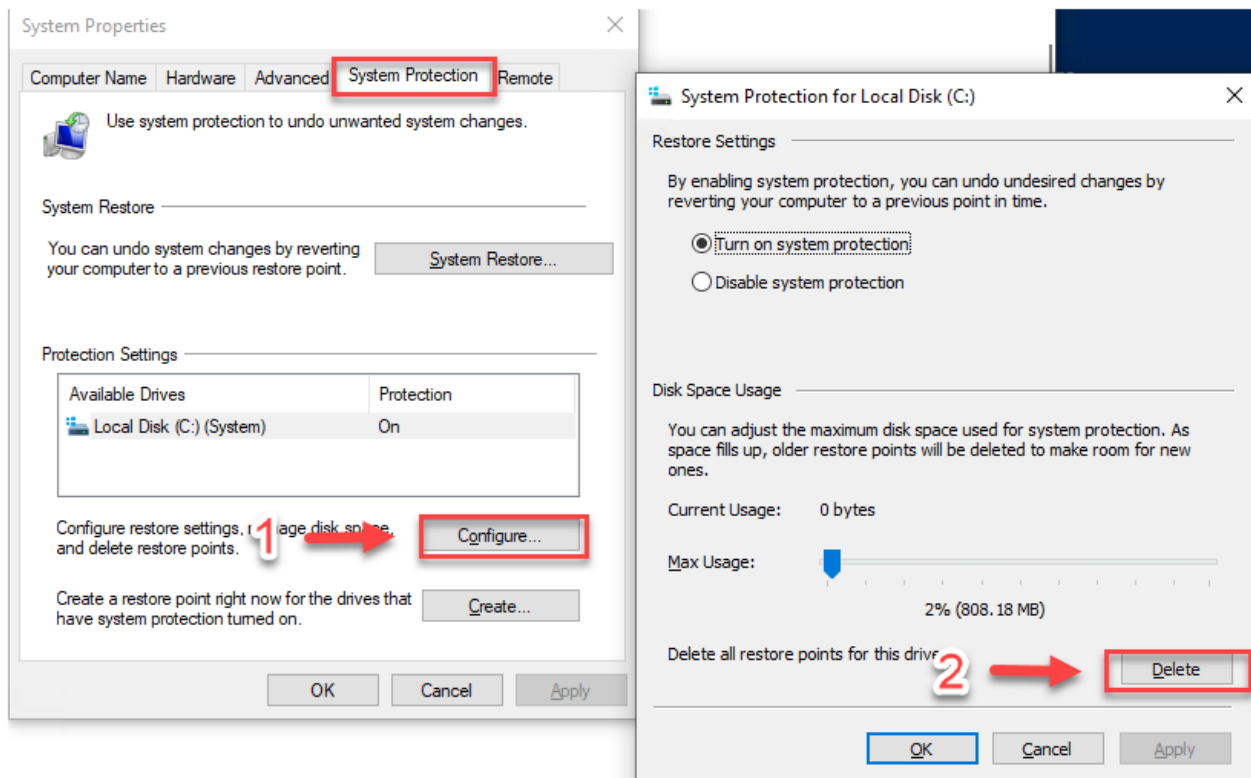
No items found that satisfy the query.
```

+ **Cách 2:** Sử dụng giao diện

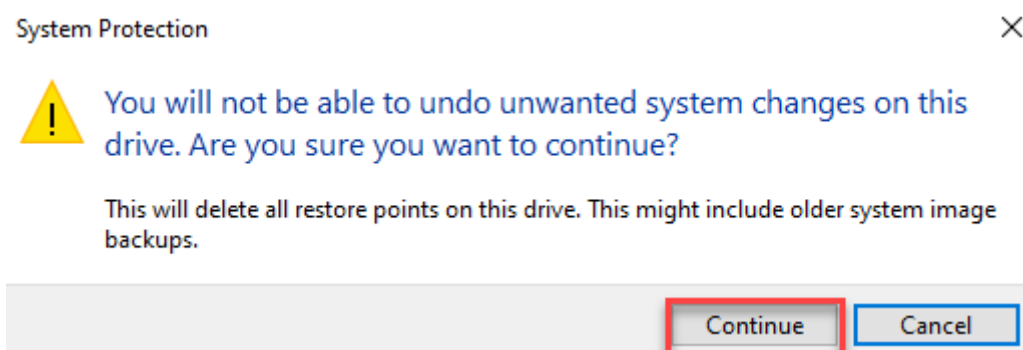
*** Truy cập Setting > nhập vào ô tìm kiếm System protect > Chọn mục Create a restore point**



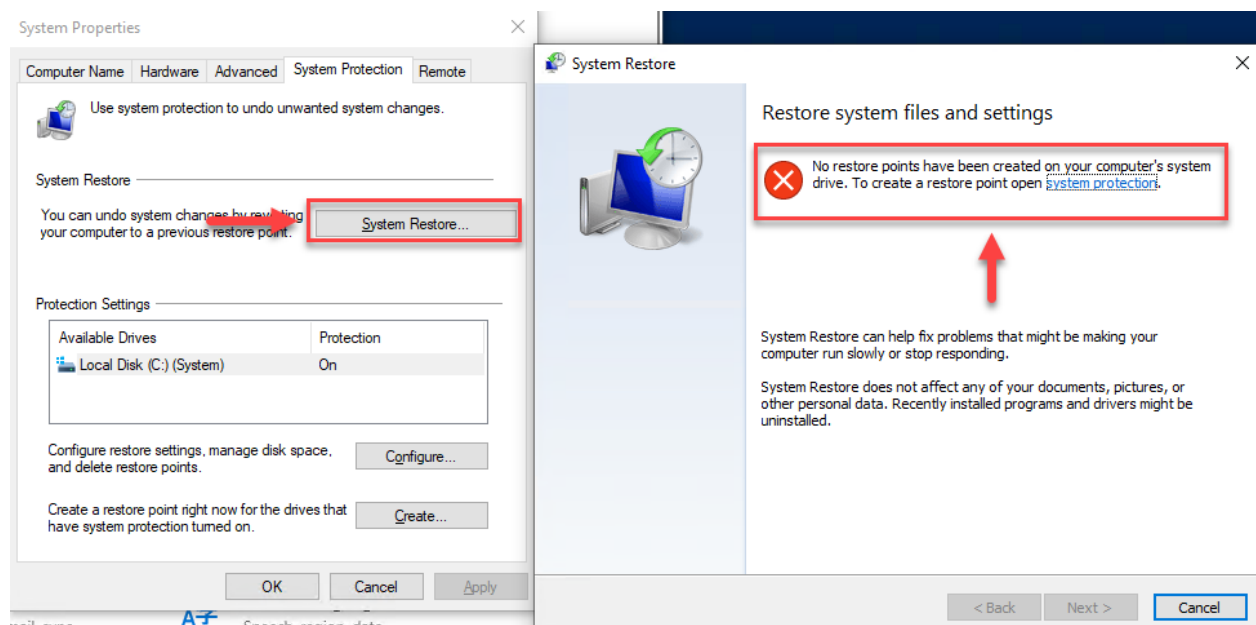
*** Tại tab System Protection > Chọn Configure > chọn Delete tại Delete all restore points for this drive trên cửa sổ pop-up mới hiện lên**



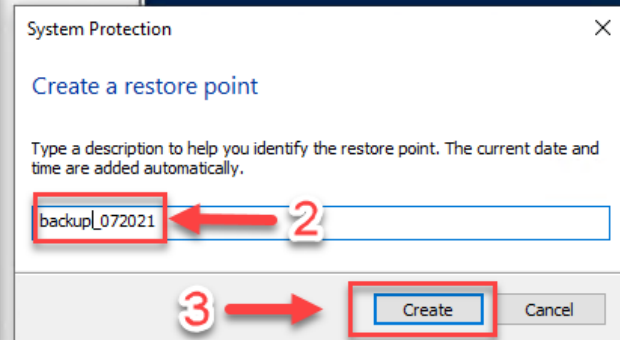
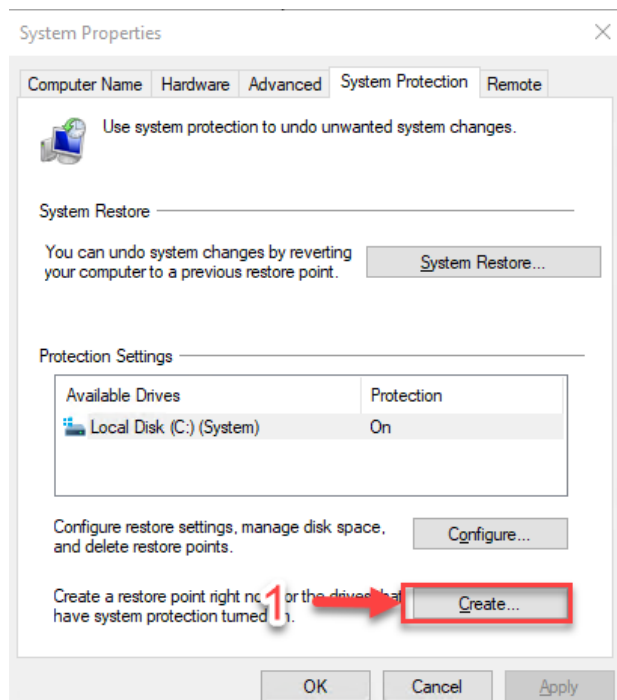
* Chọn **Continue** để hoàn tất việc xóa các bản sao



* **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:

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

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Thanh tra Bộ
2.	Cục Công tác phía Nam
3.	Cục Ứng dụng và phát triển công nghệ
4.	Cục Năng lượng nguyên tử
5.	Cục Thông tin Khoa học và Công nghệ Quốc gia
6.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
7.	Cục An toàn bức xạ và hạt nhân
8.	Cục Sở hữu trí tuệ
9.	Tổng Cục tiêu chuẩn đo lường chất lượng
10.	Ban quản lý khu công nghệ cao Hoà Lạc
11.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
12.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
13.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
14.	Viện Năng lượng nguyên tử Việt Nam
15.	Viện Ứng dụng công nghệ
16.	Viện Đánh giá khoa học và Định giá công nghệ
17.	Viện Khoa học sở hữu trí tuệ
18.	Viện Nghiên cứu và Phát triển Vùng
19.	Văn phòng các Chương trình trọng điểm cấp nhà nước
20.	Văn phòng Công nhận chất lượng
21.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
22.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
23.	Báo Khoa học và Phát triển
24.	Tạp chí Khoa học và Công nghệ Việt Nam
25.	Nhà xuất bản Khoa học và Kỹ thuật
26.	Quỹ Phát triển khoa học và công nghệ quốc gia
27.	Quỹ Đổi mới công nghệ quốc gia
28.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
29.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế