UBND TỈNH SÓC TRĂNG
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

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

Số: 1324 /STTTT-CNTT
V/v lỗ hổng bảo mật CVE-2021-40444 trong Microsoft Windows

*Sóc Trăng, ngày 16 tháng 9 năm 2021*

Kính gửi:
- Sở, ngành tỉnh;
- Ban quản lý các Khu công nghiệp tỉnh;
- Ban quản lý Dự án 1;
- Ban quản lý Dự án 2;
- UBND các huyện, thị xã, thành phố, tỉnh Sóc Trăng.

Căn cứ Công văn số 1229/CATTT-NCSC ngày 10/9/2021 của Cục An toàn thông tin về việc lỗ hổng bảo mật CVE-2021-40444 trong Microsoft Windows,

Hiện tại, lỗ hổng bảo mật này đã có mã khai thác công khai trên Internet, có thể dùng với nhiều kịch bản tấn công vào người dùng khác nhau với khả năng thành công rất cao. Sở Thông tin và Truyền thông nhận thấy mức độ ảnh hưởng của lỗ hổng này rất lớn, có nguy cơ tấn công trên diện rộng và là mục tiêu của các đối tượng tấn công mạng có chủ đích (APT).

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các đơn vị. Sở Thông tin và Truyền thông đề nghị các đơn vị thực hiện:

1. Kiểm tra, rà soát và xác định các máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Tại thời điểm hiện tại chưa có thông tin bản vá cho lỗ hổng bảo mật trên, vì vậy để giảm thiểu nguy cơ tấn công, Quý đơn vị thực hiện biện pháp khắc phục theo hướng dẫn của Microsoft *(chi tiết tham khảo tài liệu hướng dẫn kèm theo).*

2. Tăng cường các công cụ bảo vệ, công cụ giám sát, phần mềm phòng chống mã độc cho toàn bộ máy tính của người dùng. Hiện nay, công cụ Microsoft
Defender Antivirus và Microsoft Defender for Endpoint đều có khả năng phát hiện và ngăn chặn lỗ hổng này.

3. 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 quá trình thực hiện nếu có khó khăn, vướng mắc xin liên hệ số điện thoại 0299.3626600 gặp ông Trương Gia Bảo hoặc gửi về địa chỉ email tgbao@soctrang.gov.vn.

Trân trọng !

***Nơi nhận:***
- Như trên;
- Lưu: VT, CNTT.

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH SÓC TRĂNG

Sở Thông tin và Truyền thông
Tỉnh Sóc Trăng
16-09-2021 08:10:52 +07:00

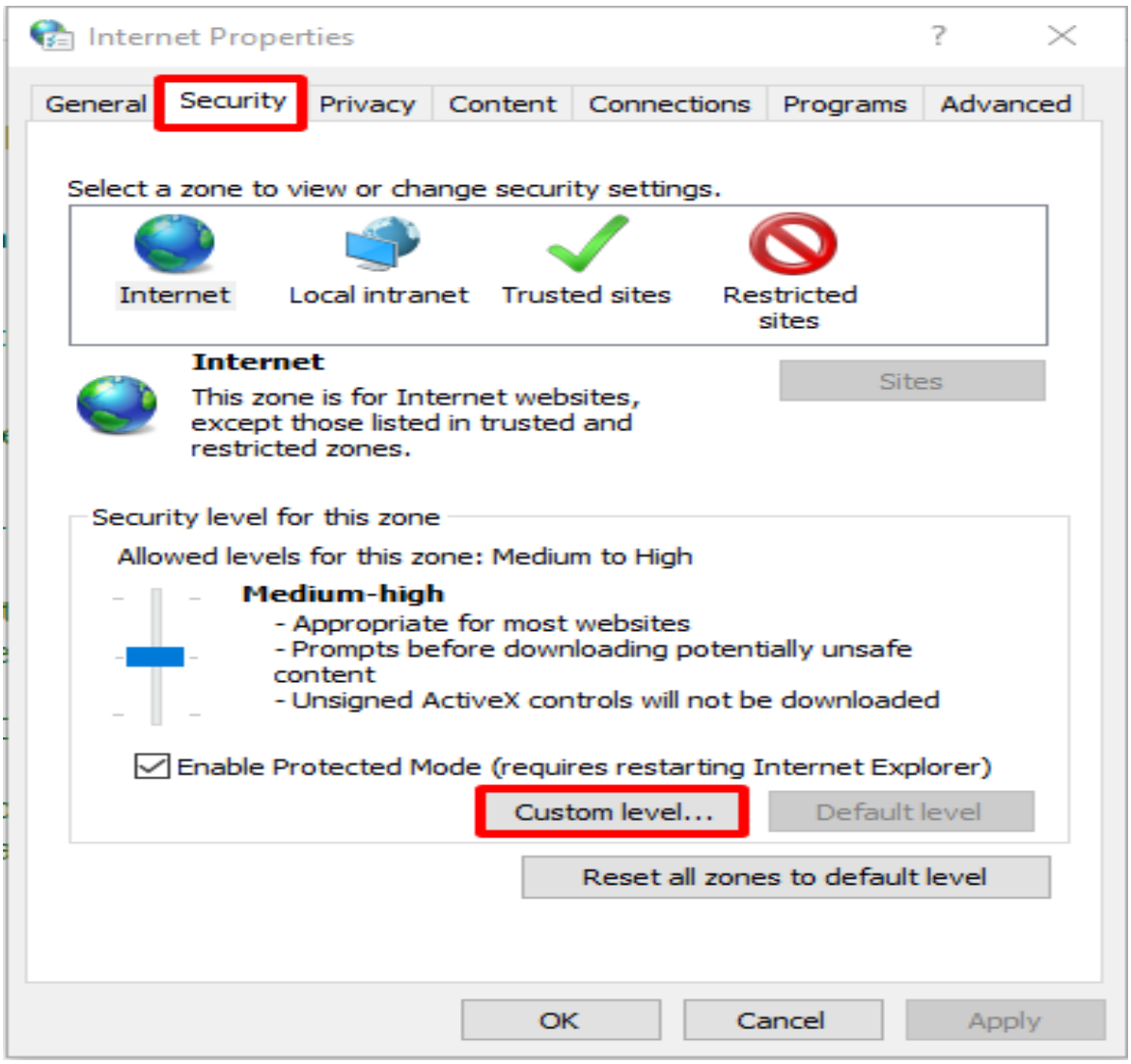
**Dương Văn Nhân**

# TÀI LIỆU HƯỚNG DẪN

*(Đính kèm Công văn số.1324../STTTT-CNTT ngày....16../9/2021 của Sở Thông tin và Truyền thông tỉnh Sóc Trăng)*

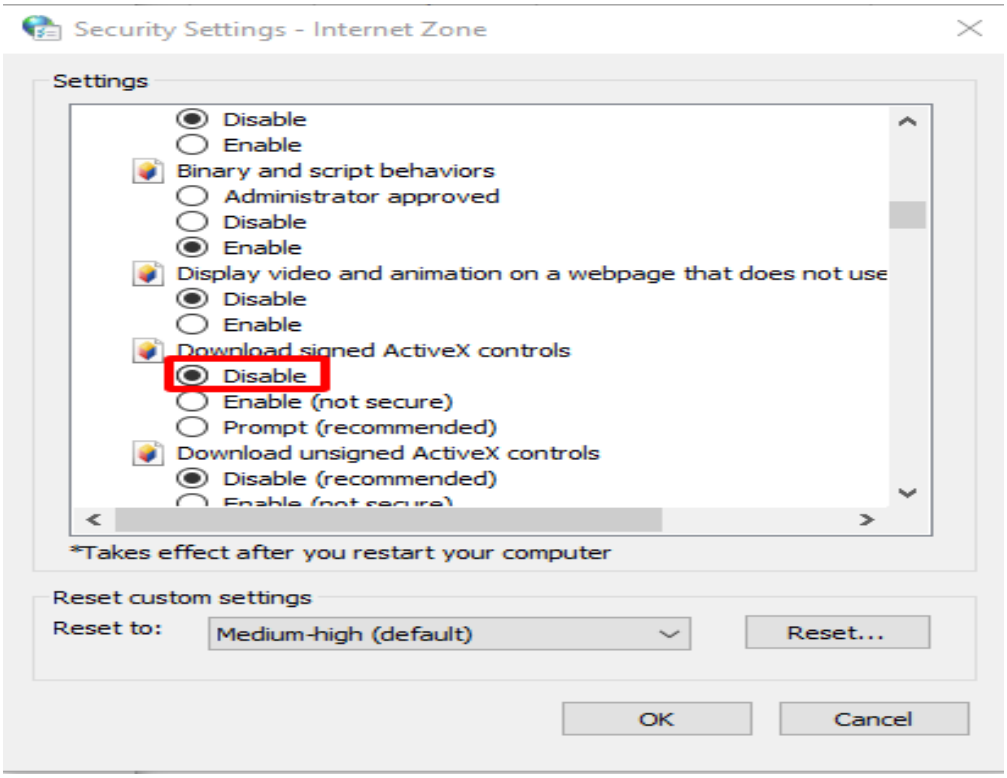
## I. Vô hiệu hóa ActiveX controls thông qua Group Policy:

**Bước 1**: Chọn control panel → internet Options → security → custom level



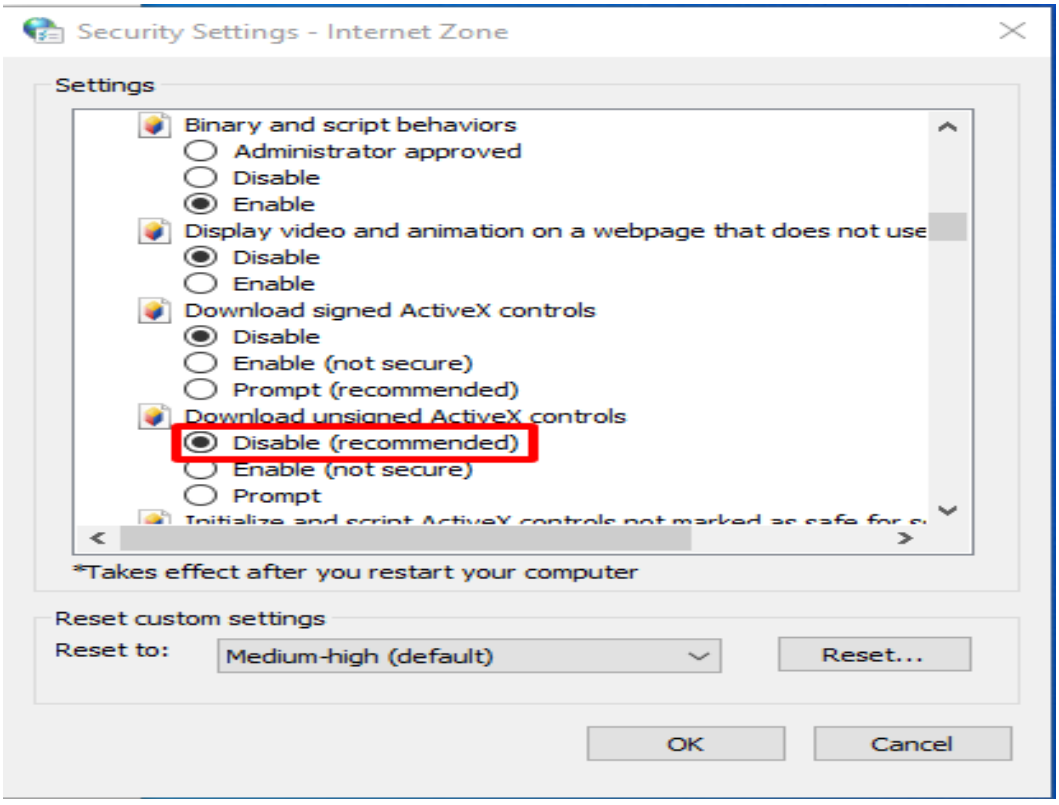

**Bước 2**: Nhấn đúp vào **Download signed ActiveX controls** và **Enable** phần policy.

Trong phần tùy chọn, nhấn vào **Disable**.




**Bước 3:** Nhấn đúp vào **Download unsigned ActiveX controls** và **Enable** phần policy.

Trong phần tùy chọn, nhấn vào **Disable**.



## II. Vô hiệu hóa ActiveX controls thông qua regkey

**Bước 1:** Để vô hiệu hóa cài đặt ActiveX controls trong Internet Explorer ở tất cả các zone, hãy dán phần sau vào file text và lưu nó với phần mở rộng file .reg:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Curre
ntVersion\I
nternet Settings\Zones\0]
"1001"=dword:00000003
"1004"=dword:00000003
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Curre
ntVersion\I
nternet Settings\Zones\1]
"1001"=dword:00000003
"1004"=dword:00000003
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Curre
ntVersion\I
nternet Settings\Zones\2]
"1001"=dword:00000003
"1004"=dword:00000003
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Curre
ntVersion\I
nternet Settings\Zones\3]
"1001"=dword:00000003
"1004"=dword:00000003
```

**Bước 2:** Nhấn đúp vào file .reg để áp dụng nó vào Policy hive.

**Bước 3:** Khởi động lại hệ thống.

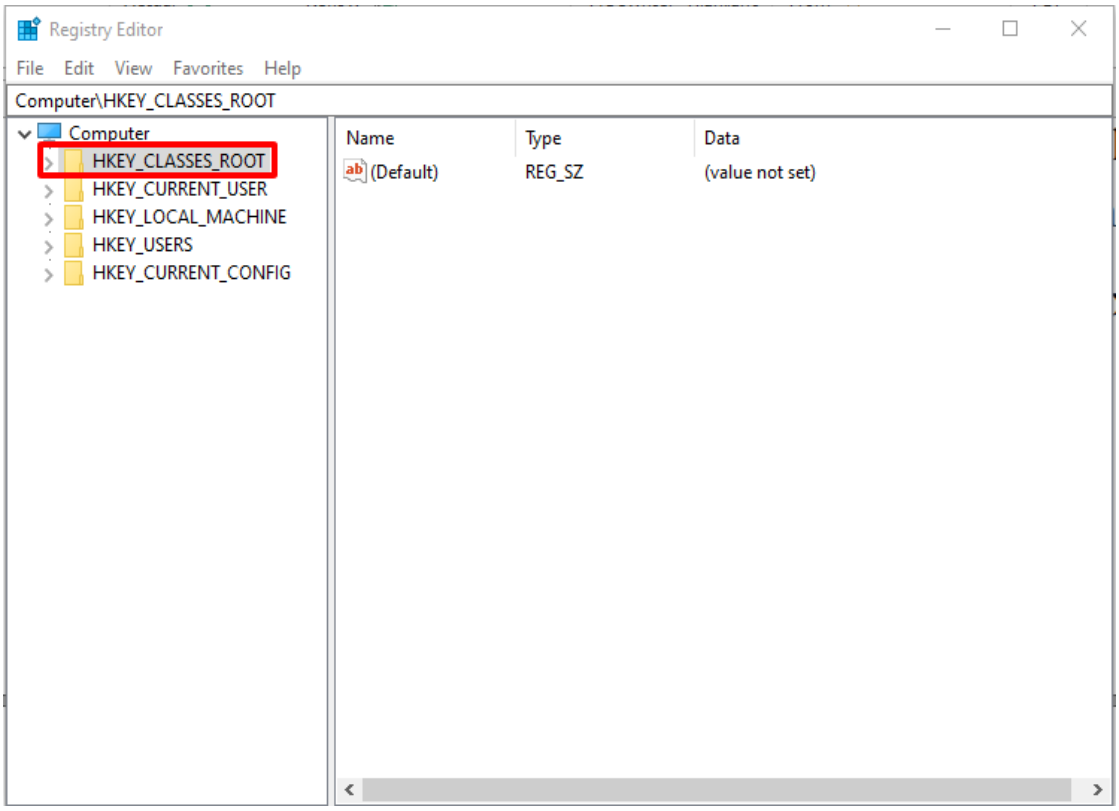
## III. Vô hiệu hóa tính năng xem trước trong Windows Explorer

Tắt Shell Preview ngăn người dùng xem trước tài liệu trong Windows Explorer. Thực hiện các bước như sau đối với từng tài liệu muốn ngăn chặn xem trước

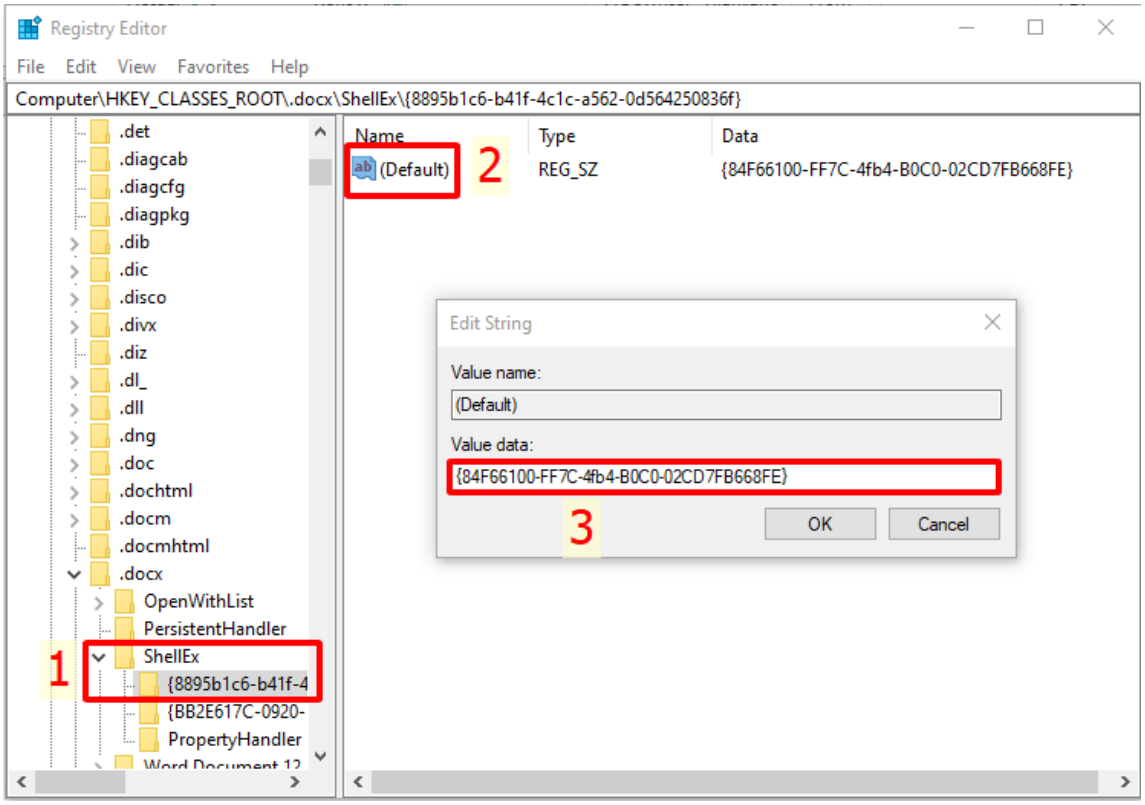
**Bước 1:** Trong Registry Editor, chọn registry key phù hợp:

- Đối với tài liệu Word:

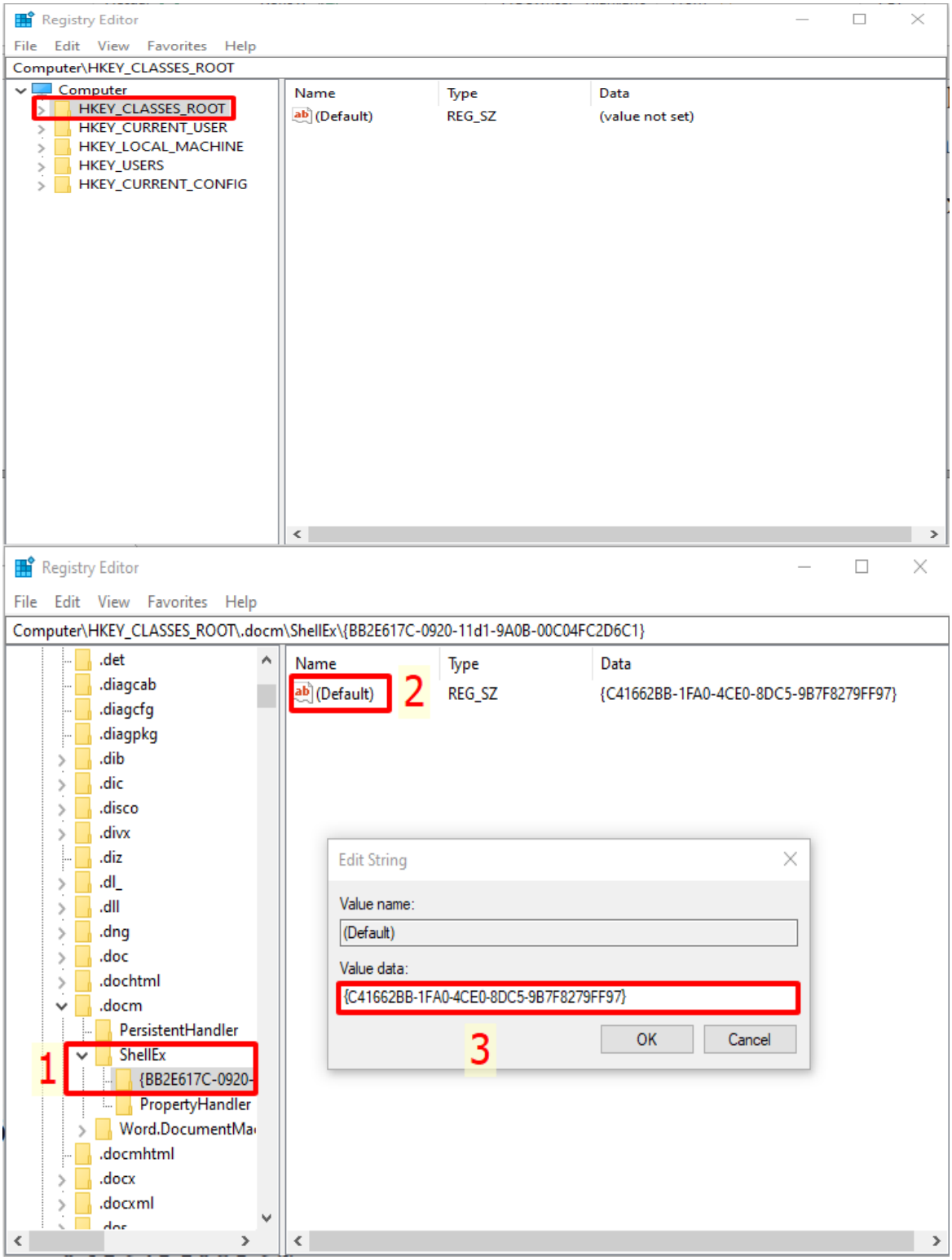
- HKEY_CLASSES_ROOT.docx \ ShellEx {8895b1c6-b41f-4c1c-a562-0d564250836f}




- HKEY_CLASSES_ROOT.doc \ ShellEx {8895b1c6-b41f-4c1c-a562-0d564250836f}

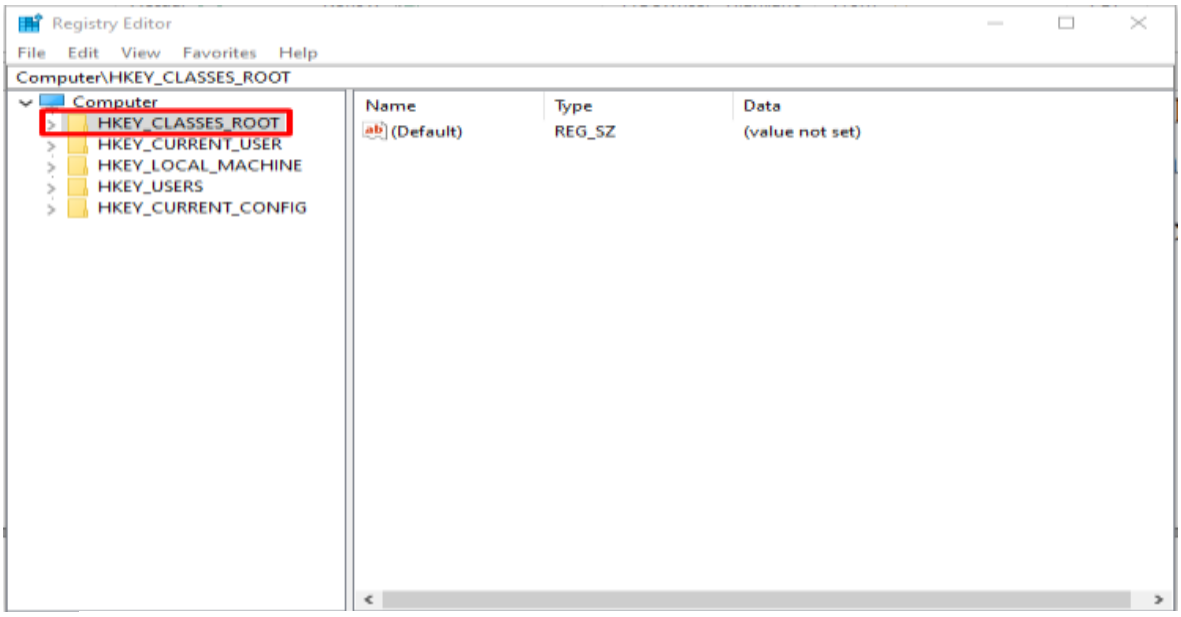


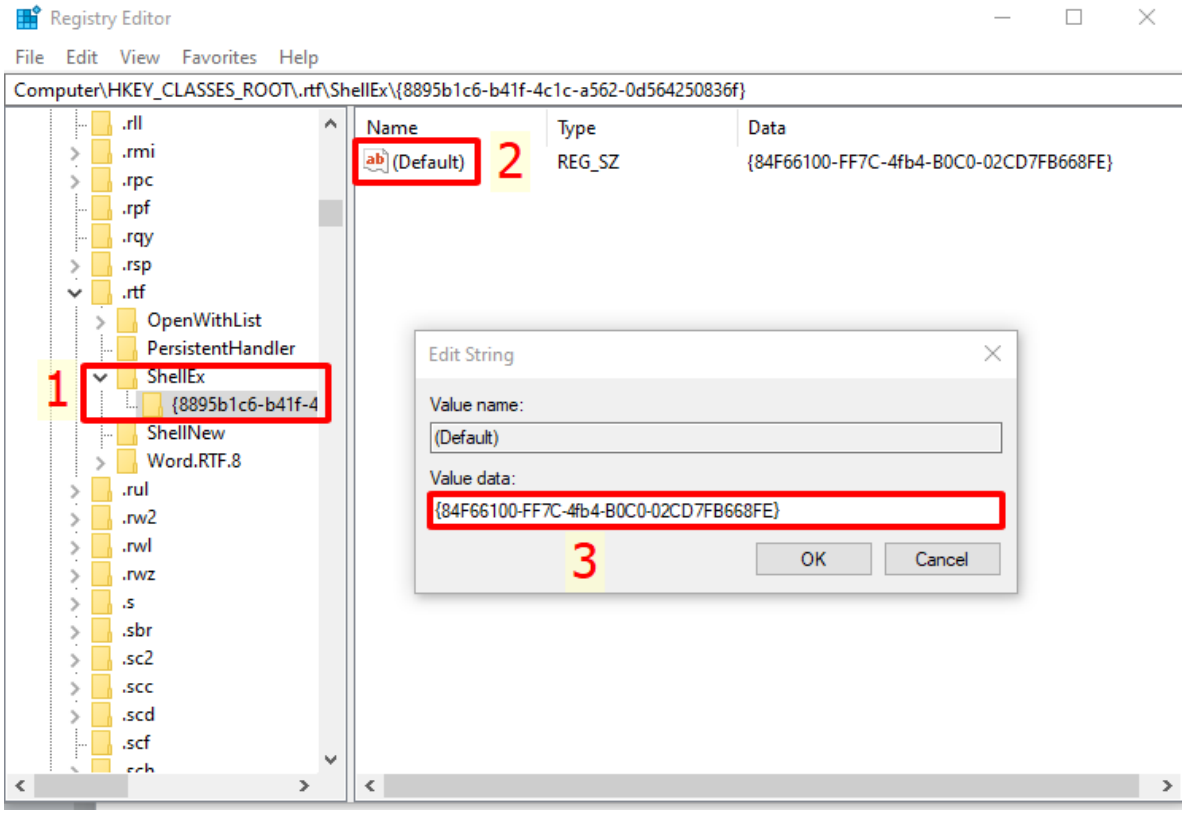
• HKEY_CLASSES_ROOT.docm \ ShellEx {8895b1c6-b41f-4c1c-a562-0d564250836f}




- Đối với file text:

•HKEY_CLASSES_ROOT.rtf\ShellEx{8895b1c6-b41f-4c1c-a562-0d564250836f}




**Bước 2:** Sao lưu 1 bản regkey

**Bước 3:** Nhấp đúp vào **Name** và trong hộp thoại **Edit String**, hãy xóa Value Data.

**Bước 4:** Chọn **OK.**

## IV. Nguồn tham khảo

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444