

Số: /TTCNTTTT-KTCCN

Cao Bằng, ngày tháng 9 năm 2021

V/v cảnh báo lỗ hổng bảo mật CVE-2021-40444 trong Microsoft Windows

Kính gửi:

- Văn phòng Tỉnh uỷ;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành, UBND các huyện và thành phố;
- Tòa án nhân dân tỉnh, Viện kiểm sát nhân dân tỉnh;
- Cục thuế tỉnh, Cục Hải quan tỉnh, Cục Quản lý thị trường tỉnh, Bảo hiểm xã hội tỉnh.

Thực hiện chức năng, nhiệm vụ được giao, qua hoạt động điều phối, hợp tác và chia sẻ thông tin của Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia, Trung tâm Công nghệ thông tin và Truyền thông Cao Bằng nhận được cảnh báo tại Công văn số 1229/CATTT-NCSC ngày 10/9/2021 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc lỗ hổng bảo mật CVE-2021-40444 trong Microsoft Windows.

Ngày 7/9/2021 vừa qua, Microsoft vừa công bố lỗ hổng bảo mật **CVE-2021-40444** trong Microsoft Windows, ảnh hưởng đến các phiên bản Windows 7/8/8.1/RT/10, Windows Server 2008/2012/2016/2019/2022. Lỗ hổng này có điểm CVSS: 8.8 (cao), cho phép đối tượng tấn công thực thi mã từ xa trong MSHTML. MSHTML là một thành phần của hệ điều hành được dùng bởi khá nhiều chương trình của Microsoft như: Microsoft Office, bao gồm Word và PowerPoint, ....

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. Vì vậy, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin nhận thấy mức độ ảnh hưởng của lỗ hổng này khá lớn, có nguy cơ tấn công trên diện rộng và là mục tiêu nhằm đến của các đối tượng tấn công mạng có chủ đích (APT).

Nhằm đảm bảo an toàn thông tin cho hệ thống của quý đơn vị, Trung tâm Công nghệ thông tin và Truyền thông kính đề nghị quý cơ quan, đơn vị thực hiện một số nội dung sau:

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 tại phụ lục 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 trường hợp cần thiết có thể liên hệ đầu mối ứng cứu sự cố máy tính tỉnh Cao Bằng: Trung tâm Công nghệ thông tin và Truyền thông Cao Bằng, Địa chỉ: Số 009, Hoàng Văn Thụ, Hợp Giang, thành phố Cao Bằng, Điện thoại: 02063.955.899. Email: cbitc@caobang.gov.vn.

Đề nghị quý cơ quan, đơn vị quan tâm triển khai thực hiện./.

**GIÁM ĐỐC**

***Nơi nhận:***

- Như trên;
- Lãnh đạo Sở TTTT (b/c);
- Phòng BCVT-CNTT;
- Lưu: VT, KTCN.

**Triệu Đình Thăng**

## Phụ lục

### Thông tin lỗ hổng bảo mật

(Kèm theo Công văn số: /TTCNTTTT-KTCCN ngày /9/2021  
của Trung tâm Công nghệ thông tin và Truyền thông Cao Bằng)

#### 1. Thông tin lỗ hổng bảo mật

- **Mô tả:** Lỗ hổng tồn tại trong MSHTML của Microsoft Windows, cho phép đối tượng tấn công thực thi mã từ xa.

- **Điểm CVSS:** 8.8 (cao)

- **Ảnh hưởng:** các phiên bản Windows 7/8/8.1RT/10, Windows Server 2008/2012/2016/2019/2022.

#### 2. Hướng dẫn khắc phục

Tại thời điểm hiện tại chưa có thông tin bản vá cho lỗ hổng bảo mật, tuy nhiên Microsoft có đưa ra biện pháp khắc phục để giảm thiểu nguy cơ tấn công bởi lỗ hổng này bằng cách vô hiệu hóa tất cả các cài đặt ActiveX controls trong Internet Explorer.

Các bước thực hiện như sau:

##### **Vô hiệu hóa ActiveX controls thông qua Group Policy:**

**Bước 1:** Trong phần cài đặt Group Policy, chọn Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page

##### **Bước 2:** Đối với mỗi Zone

1. Chọn Zone (Internet Zone, Intranet Zone, Local Machine Zone hoặc Trusted Sites Zone)

2. Nhấn đúp vào **Download signed ActiveX controls** và **Enable** phần policy. Trong phần tùy chọn, nhấn vào **Disable**.

3. Nhấn đúp vào **Download unsigned ActiveX controls** và **Enable** phần policy. Trong phần tùy chọn, nhấn vào **Disable**.

Microsoft khuyến nghị nên áp dụng cài đặt này cho tất cả các khu vực để bảo vệ toàn bộ hệ thống đang sử dụng.

##### **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\CurrentVersion\Internet Settings\Zones\0]
```

```
"1001"=dword:00000003
```

```
"1004"=dword:00000003
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1]
```

```
"1001"=dword:00000003
```

```
"1004"=dword:00000003
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2]
```

```
"1001"=dword:00000003
```

```
"1004"=dword:00000003
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet 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.

### **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**.

### **3. Nguồn tham khảo**

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