ỦY BAN NHÂN DÂN **THÀNH PHỐ PHỦ LÝ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số:1321 /UBND-VHTT V/v lỗ hổng bảo mật CVE-2021-40444 trong Microsoft Windows	*Phủ Lý, ngày 20 tháng 9 năm 2021*

Kính gửi:
- Các phòng, ban, ngành, đoàn thể thuộc Thành phố;
- UBND các phường, xã.

Căn cứ công văn số 918/STTTT-BCVTCNTT ngày 13/9/2021 của Sở Thông tin và Truyền thông tỉnh Hà Nam về việc lỗ hổng bảo mật CVE-202140444 trong Microsoft Windows.

Nhằm tăng cường công tác bảo đảm an toàn, an ninh thông tin, đặc biệt là bảo vệ các hệ thống thông tin của các cơ quan, đơn vị trên địa bàn, UBND Thành phố yêu cầu các đơn vị, phòng, ban, UBND các phường, xã thực hiện nội dung sau:

1. Kiểm tra, rà soát và xác định các máy sử dụng hệ điều hành Windows có 2 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, đề nghị các cơ quan, đơn vị thực hiện biện pháp khắc phục theo hướng dẫn của Microsoft (*Chi tiết hướng dẫn 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.

Đầu mối liên hệ, hỗ trợ

- Trung tâm Công nghệ thông tin và Truyền thông - Bộ phận thường trực Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Nam. Điện thoại: **0226.3846333**. Email: ttcntt@hanam.gov.vn

- Trung tâm Giám sát an toàn thông tin mạng quốc gia (NCSC), Cục An toàn thông tin. Điện thoại: **0243.2091616**. Email: **ais@mic.gov.vn**

Nơi nhận: - Sở TT&TT (để b/c); - Lãnh đạo UBND TP; - Các phòng, ban, ngành, đoàn thể; - UBND các phường, xã; - Lưu: VT,VHTT.	**TM. ỦY BAN NHÂN DÂN** **KT. CHỦ TỊCH** **PHÓ CHỦ TỊCH** **Phạm Văn Quân**

PHỤ LỤC

Thông tin và hướng dẫn khắc phục lỗ hổng bảo mật CVE-2021-40444 trong Microsoft Windows

(Kèm theo Công văn số /UBND-VHTT ngày /9/2021 của UBND thành phố Phủ Lý)

1. Thông tin về các lỗ hổng

- 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)

- Sản phẩm bị ảnh hưởng: Các phiên bản Windows 7/8/8.1RT/10, Windows Server 2008/2012/2016/2019/2022.

2. Hướng dẫn khắc phục

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 về 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