BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

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

Số: 260 /TTCNTT-KTHT
V/v: lỗ hổng bảo mật CVE-2021-40444 trong Microsoft Windows

Hà Nội, ngày 14 tháng 09năm 2021

Kính gửi: Các đơn vị trực thuộc Bộ

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 7/8/8.1RT/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 Công nghệ 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 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 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, 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: phongktht@most.gov.vn.

Trân trọng./.

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

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục

Thông tin các lỗ hổng bảo mật

(Kèm theo Công văn số 260 /TTCNTT-KTHT ngày 14 /09 /2021 của Trung tâm Công nghệ thông tin)

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 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\I nternet Settings\Zones\0]*
  "1001"=dword:00000003
  "1004"=dword:00000003
- *[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\I nternet Settings\Zones\1]*
  "1001"=dword:00000003
  "1004"=dword:00000003
- *[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\I nternet Settings\Zones\2]*
  "1001"=dword:00000003
  "1004"=dword:00000003
- *[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\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.

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

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 260 /TTCNTT-KTHT ngày 14 /09/2021 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 Hòa 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