|  |  |
| --- | --- |
| UBND TỈNH TÂY NINH  **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**  Số: /STTTT-TTGSĐH  V/v cảnh báo và khắc phục lỗ hổng bảo mật  HĐH Window CVE-2021-40444 | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập – Tự do – Hạnh phúc**  *Tây Ninh, ngày tháng 9 năm 2021* |

Kính gửi:

- Văn phòng Tỉnh ủy;

- Văn phòng Đoàn ĐBQH và HĐND tỉnh;

- Văn phòng UBND tỉnh;

- Các Sở, ban, ngành tỉnh;

- UBND các huyện, thị xã, thành phố.

Thực hiện theo Công văn số 1229/CATTT-NCSC ngày 10/9/2021 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật mới ảnh hưởng đến hệ điều hành Windows CVE-2021-40444. Mã lỗ hổng này cho phép 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 nhiều chương trình của Microsoft như: Microsoft Office, bao gồm Word và PowerPoint,…

Do đó, để đảm bảo an toàn thông tin cho hệ thống thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương chủ trì, chỉ đạo thực hiện gấp các công việc cụ thể như sau:

1. Rà soát, kiểm tra cho cácmáy tính/máy chủ nếu nằm trong phạm vi ảnh hưởng của lỗ hổng bảo mật và tiến hành khắc phục *(Phụ lục hướng dẫn kèm theo)*.
2. Tăng cường kiểm tra, giám sát hệ thống mạng của đơn vị, địa phương, khi có phát hiện hoạt động tấn công mạng, đề nghị liên hệ Sở Thông tin và Truyền thông để phối hợp xử lý kịp thời.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

|  |  |
| --- | --- |
| ***Nơi nhận:***  - Như trên;  - Lưu: VT, TTGSĐH. | **KT. GIÁM ĐỐC**  **PHÓ GIÁM ĐỐC** |

# PHỤ LỤC

**HƯỚNG DẪN KHẮC PHỤC LỖ HỔNG BẢO MẬT**

**CVE-2021-36934**

**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.

- **Đánh giá mức độ:** 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)

**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.** 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 WindowsExplorer.

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>