ỦY BAN NHÂN DÂN **HUYỆN HÀ QUẢNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 3992 /UBND-VHTT V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2021	*Hà Quảng, ngày 25 tháng 12 năm 2021*

Kính gửi:
- Các cơ quan, ban ngành đoàn thể huyện;
- UBND các xã, thị trấn.

(gọi chung là các cơ quan, đơn vị)

Thực hiện Công văn số 206/TTCNTTTT- KTCGCN ngày 20 tháng 12 năm 2021 của Trung tâm Công nghệ thông tin và Truyền thông, về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2021.

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 1749/CATTT-NCSC ngày 15/12/2021 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2021.

Tháng 12/2021, Microsoft đã phát hành danh sách bản vá 67 lỗ hổng bảo mật của hãng, trong đó có một số lỗ hổng như sau:

1. Lỗ hổng Đặc biệt nghiêm trọng

- Lỗ hổng bảo mật **CVE-2021-43907** trong Windows Subsystem for Linux (WSL *là một tính năng có trên Windows x64 cho phép chạy hệ điều hành Linux trên Windows*), cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2021-43899** trong Microsoft 4K Wireless Display Adapter, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2021-43215** trong iSNS Server, cho phép đối tượng tấn công thực thi mã từ xa

2. Lỗ hổng có mức ảnh hưởng cao

- Lỗ hổng bảo mật **CVE-2021-43890** trong Windows AppX Installer, cho phép đối tượng tấn công thực hiện tấn công giả mạo. Bên cạnh đó, lỗ hổng này được cho là đang được khai thác trong chiến dịch tấn công mã độc Emotet, Trickbot, Bazaloader.

- Lỗ hổng bảo mật **CVE-2021-42309** trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2021-41333** trong Windows Print Spooler, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2021-43880** trong Windows Mobile Device Management, cho phép đối tượng tấn công nâng cao đặc quyền, xóa tệp tin trong hệ thống mục tiêu.

- Lỗ hổng bảo mật **CVE-2021-43893** trong Windows Encrypting File System (EFS), cho phép đối tượng tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2021-43240** trong NTFS Set Short Name, cho phép đối tượng tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2021-43883** trong Windows Installer cho phép đối tượng tấn công leo thang đặc quyền.

(*Thông tin chi tiết điểm yếu, lỗ hổng và hướng dẫn khắc phục có tại phụ lục kèm theo Công văn số 1749/CATTT-NCSC ngày 15/12/2021 của Cục An toàn thông tin được gửi kèm)*

Nhằm đảm bảo an toàn thông tin cho hệ thống của các đơn vị, Ủy ban nhân dân huyện đề nghị các cơ quan, đơn vị thực hiện một số nội dung sau:

1. Kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công.

2. 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 các cơ quan đơn vị, Ủy ban nhân dân các xã, thị trấn phối hợp triển khai thực hiện./.

Nơi nhận:
- Như trên (VB điện tử);
- Chủ tịch, các PCT UBND huyện;
- Lưu: VT, VHTT (Oanh Tuấn, Bắc).

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Ký bởi: Ủy ban nhân dân huyện Hà Quảng
Thời gian ký: 25/12/2021 14:59:57

Nguyễn Thị Phương