ỦY BAN NHÂN DÂN **HUYỆN HÀ QUẢNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 662 /UBND-VHTT V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2022	*Hà Quảng, ngày 14 tháng 3 năm 2022*

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 31/TTCNTTTT- KTCGCN ngày 11 tháng 3 năm 2022 của Trung tâm Công nghệ thông tin và Truyền thông về cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2022.

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 315/CATTT-NCSC ngày 09/3/2022 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 3/2022.

Tháng 3/2022, Microsoft đã phát hành danh sách bản vá **71** lỗ hổng bảo mật của hãng, trong đó có một số lỗ hổng bảo mật có mức ảnh hưởng cao như sau:

- 02 lỗ hổng bảo mật **CVE-2022-21990, CVE-2022-23285** trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã có mã khai thác được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật **CVE-2022-24459** trong Windows Fax và Scan Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-24508** trong SMBv3 cho phép đối tượng tấn công thực thi mã từ xa trên Windows SMBv3 Client/Server.

- Lỗ hổng bảo mật **CVE-2022-23277** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ.

- Lỗ hổng bảo mật **CVE-2022-21967** trong Xbox Live Auth Manager for Windows cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-22006** trong HEVC Video Extensions cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-24501** trong cho phép đối tượng tấn công thực thi mã từ xa.

(*Thông tin chi tiết điểm yếu, lỗ hổng và hướng dẫn khắc phục có tại phụ lục kèm theo Công văn số 315/CATTT-NCSC ngày 09/03/2022 của Cục An toàn thông tin được gửi kèm)*

Nhằm đảm bảo an toàn thông tin cho hệ thống của các cơ quan đơn vị, Ủy ban nhân 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.

Ủy ban nhân dân huyện đề nghị các cơ quan đơn vị, Ủy ban nhân dân các xã, thị trấn phối hợp chỉ đạo 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: 14/03/2022 15:05:50

Nguyễn Thị Phương