SỞ THÔNG TIN VÀ TRUYỀN THÔNG
CAO BẰNG
**TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

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

Số: 115 /TTCNTTTT-KTCN

V/v cảnh báo 05 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft

*Cao Bằng, ngày 21 tháng 7 năm 2021*

Kính gửi:

- Văn phòng Tỉnh uỷ;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành, UBND các huyện và thành phố;
- Toà án nhân dân tỉnh, Viện kiểm sát nhân dân tỉnh;
- Cục thuế tỉnh, Cục Hải quan tỉnh, Cục Quản lý thị trường tỉnh, Bảo hiểm xã hội tỉnh.

Thực hiện chỉ đạo của Lãnh đạo UBND tỉnh tại Công văn số 1384/VP-VX ngày 19/07/2021 về việc xử lý lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft và triển khai nhiệm vụ được giao về hoạt động điều phối, hợp tác và chia sẻ thông tin, ứng cứu sự cố mạng máy tính trên địa bàn tỉnh. Trung tâm Công nghệ thông tin và Truyền thông - Sở Thông tin và Truyền thông nhận được cảnh báo tại Công văn số 2604/BTTTT-CATTT ngày 16/07/2021 của Bộ Thông tin và Truyền thông về việc 05 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft. Các lỗ hổng bảo mật gồm:

- Lỗ hổng **CVE-2021-34473, CVE-2021-34523**: tồn tại trong Microsoft Exchange Server, cho phép đối tượng tấn công có thể thực thi mã từ xa, nâng cao đặc quyền trên máy chủ thư điện tử.

- Lỗ hổng **CVE-2021-34527**: thực thi mã từ xa thứ 2 trong Windows Print Spooler (*liên quan đến lỗ hổng CVE-2021-1675 – đã được cảnh báo trong công văn số 100/TTCNTTTT- KTCGCN ngày 02/07/2021 của Trung tâm Công nghệ thông tin và Truyền thông Cao Bằng*).

- Lỗ hổng **CVE-2021-33781**: lỗ hổng cho phép đối tượng có đặc quyền thấp tấn công từ xa vượt qua các cơ chế kiểm tra bảo mật trong dịch vụ Active Directory để đạt được các đặc quyền cao hơn trên máy mục tiêu.

- Lỗ hổng **CVE-2021-34492:** lỗ hổng cho phép đối tượng tấn công vượt qua cơ chế kiểm tra trong Windows Certificate để giả mạo chứng chỉ. Lỗ hổng này là hoàn toàn có thể được dùng trong các cuộc tấn công khác nhằm vào người dùng.

(*Thông tin chi tiết điểm yếu, lỗ hổng và hướng dẫn khắc phục có tại phụ lục kèm theo Công văn số 2604/BTTTT-CATTT ngày 16/07/2021 của Bộ Thông tin và Truyền thông được gửi kèm*).

Nhằm đảm bảo an toàn thông tin cho hệ thống của quý đơn vị, Trung tâm Công nghệ thông tin và Truyền thông kính đề nghị quý cơ quan, đơn vị thực hiện một số nội dung sau:

1. Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo hướng dẫn của Microsoft.

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 quý cơ quan, đơn vị quan tâm triển khai thực hiện./.

***Nơi nhận:***
- Như trên;
- Lãnh đạo Sở TTTT (b/c);
- Phòng BCVT-CNTT;
- Lưu: VT, KTCGCN.

**GIÁM ĐỐC**

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH CAO BẰNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

**Triệu Đình Thăng**