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: 19/TTCNTTTT-KTCGCN

Cao Bằng, ngày 14 tháng 01 năm 2022

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2022

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 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 56/CATTT-NCSC ngày 12/01/2022 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 01/2022.

Tháng 01/2022, Microsoft đã phát hành danh sách bản vá 96 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-2022-21907** trong HTTP Protocol Stack (http.sys) của Windows, cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực.

2. Lỗ hổng có mức ảnh hưởng Cao

- 03 lỗ hổng bảo mật **CVE-2022-21846**, **CVE-2022-21969, CVE-2022-21855** trong Microsoft Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. Để khai thác lỗ hổng này, kẻ tấn công cần có quyền truy cập vào mạng mục tiêu từ đấy có thể chiếm quyền điều khiển máy chủ.

- Lỗ hổng bảo mật **CVE-2022-21857** trong Active Directory, cho phép đối tượng nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-21840** trong Microsoft Office, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-21911** trong .NET Framework, cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.

- Lỗ hổng bảo mật **CVE-2022-21836** trong Windows Certificate, cho phép đối tượng tấn công giả mạo.

-Lỗ hổng bảo mật **CVE-2022-21841** trong Microsoft Excel, cho phép đối tượng tấn công thực thi mã từ xa.

-Lỗ hổng bảo mật **CVE-2022-21837** trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa.

-Lỗ hổng bảo mật **CVE-2022-21842** trong Microsoft Word, 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 56/CATTT-NCSC ngày 12/01/2022 của Cục An toàn thông tin 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, 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 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