UBND TỈNH CAO BẰNG
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 2088/SGD&ĐT-QLCLCNTT
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 11/2022

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

Cao Bằng, ngày 18 tháng 11 năm 2022

Kính gửi:
- Các phòng Giáo dục và Đào tạo;
- Các trường, trung tâm trực thuộc Sở;
- Các trung tâm GDNN-GDTX.

(Gọi chung là các đơn vị)

Sở Giáo dục và Đào tạo (GD&ĐT) đã nhận được Công văn số 176/TTCNTTTT-KTCGCN ngày 17/11/2022 của Sở 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 11/2022.

Tháng 11/2022, Microsoft đã phát hành danh sách bản vá **64** lỗ hổng bảo mật của hãng, trong đó có một số lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng như sau:

- 06 lỗ hổng bảo mật CVE-2022-41082, CVE-2022-41040, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078, CVE-2022-41123 trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. Trong đó, 02 lỗ hổng CVE-2022-41082, CVE-2022-41040 đã được cảnh báo tại văn bản số 1484/CATTT-VNCERT/CC về việc cảnh báo lỗ hổng bảo mật zero-day ảnh hưởng nghiêm trọng đến Microsoft Exchange phát hành ngày 30/9/2022;

- 02 lỗ hổng bảo mật CVE-2022-41128, CVE-2022-41118 trong Windows Scripting Languages cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang bị khai thác trong thực tế;

- Lỗ hổng bảo mật CVE-2022-41091 trong Windows Mark of the Web cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật;

- Lỗ hổng bảo mật CVE-2022-41073 trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền;

- Lỗ hổng bảo mật CVE-2022-41125 trong Windows CNG Key Insolation Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền;

- 03 lỗ hổng bảo mật CVE-2022-41044, CVE-2022-41088, CVE-2022-

41039 trong Windows Point-to-Point cho phép đối tượng tấn công thực thi mã từ xa;

- 04 lỗ hổng bảo mật CVE-2022-41105, CVE-2022-41106, CVE-2022-41063, CVE-2022-41104 trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa, tấn công giả mạo (Spoofing), thực hiện tấn công vượt qua cơ chế bảo mật.

(*Thông tin chi tiết điểm yếu, lỗ hổng và hướng dẫn khắc phục có tại phụ lục kèm theo Công văn số 1842/CATTT-NCSC ngày 11/11/2022 của Cục An toàn thông tin được gửi kèm)*

Để bảo đảm an toàn thông tin cho hệ thống của các đơn vị, Sở GD&ĐT đề nghị các đơn vị triển khai, 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 đơn vị nghiêm túc thực hiện./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở;
- Các phòng Sở;
- Website Sở;
- Lưu: VT, QLCLCNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH CAO BẰNG

Lục Văn Dương