UBND TỈNH CAO BẰNG
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 475/SGDĐT-QLCLCNTT
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2023

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

Cao Bằng, ngày 21 tháng 3 năm 2023

Kính gửi:
- Phòng Giáo dục và Đào tạo các huyện, thành phố;
- Các trường trực thuộc Sở;
- Các phòng thuộc Sở;
- Các trung tâm GDNN-GDTX;
- Trung tâm GDTX tỉnh.

(Gọi chung là các đơn vị)

Sở Giáo dục và Đào tạo (GDĐT) nhận được Công văn số 74/TTCNTTTT-KTCN ngày 20/3/2023 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 3/2023. Microsoft đã phát hành danh sách bản vá **74** 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:

- Lỗ hổng bảo mật **CVE-2023-23397** trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế;

- Lỗ hổng bảo mật **CVE-2023-24880** trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế;

- Lỗ hổng bảo mật **CVE-2023-23392** trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa;

- Lỗ hổng bảo mật **CVE-2023-23415** trong Internet Control Message Protocol (ICMP) cho phép đối tượng tấn công thực thi mã từ xa;

- Lỗ hổng bảo mật **CVE-2023-23399** trong trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa;

- Lỗ hổng bảo mật **CVE-2023-23400** trong Windows DNS Server 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 383/CATTT-NCSC ngày 17/3/2023 của Cục An toàn thông tin được gửi kèm theo trên iOffice)*

Để bảo đảm an toàn thông tin trong hệ thống thông tin, Sở GDĐT 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 062, Bế Văn Đàn, 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;
- Website Sở;
- Lưu: VT, QLCLCNTT(Sự).

GIÁM ĐỐC

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

Vũ Văn Dương