UBND HUYỆN VĂN GIANG
PHÒNG GIÁO DỤC & ĐÀO TẠO

Số: 77/GD&ĐT-CNTT
V/v thông báo các lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 03/2022

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

Văn Giang, ngày 17 tháng 3 năm 2022

Kính gửi:
- Các trường Mầm non, Tiểu học, THCS trong huyện;
- Trường Tiểu học và Trung học cơ sở Phụng Công.

Theo thông báo của Cục An toàn thông tin – Bộ Thông tin và Truyền thông về lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft, với 71 lỗ hổng bảo mật trong các sản phẩm của Microsoft. Trong đó đáng chú ý các lỗ hổng bảo mật 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 về 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.

Để đảm bảo an toàn thông tin cho hệ thống thông tin, Phòng Giáo dục và Đào tạo đề nghị các nhà trường thực hiện rà soát, khắc phục lỗ hổng bảo mật trên theo khuyến nghị sau:

1. Thực hiện 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 *(tham khảo hướng dẫn kèm theo Công văn số 315/CATTT-NCSC gửi kèm).*

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.

3. Trong trường hợp cần thiết cần hỗ trợ các nhà trường liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Phòng Giáo dục và Đào tạo đề nghị các nhà trường quan tâm chỉ đạo và phối hợp tổ chức thực hiện./.

Nơi nhận:
- Như trên;
- Cổng TTĐT Phòng GD&ĐT;
- Lưu: VT, CNTT.

TRƯỞNG PHÒNG

CỘNG HÒA X.H.C.N VIỆT NAM
PHÒNG GIÁO DỤC VÀ ĐÀO TẠO
H. VĂN GIANG - T. HƯNG YÊN

Đào Thị Bích Ngọc