UBND TỈNH HƯNG YÊN
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 667/SGDĐT-VP
V/v lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2022

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

Hưng Yên, ngày 19 tháng 4 năm 2022

Kính gửi:
- Các đơn vị giáo dục trực thuộc;
- Phòng GDĐT các huyện/thị xã/thành phố;
- Trung tâm GDNN – GDTX các huyện/thị xã/thành phố;

Căn cứ Công văn số 374/STTTT-BCVTCNTT ngày 15/4/2022 của Sở Thông tin và Truyền thông Hưng Yên v/v lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2022,

Theo thông báo của Cục An toàn thông tin – Bộ Thông tin và Truyền thông về lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft, với 128 lỗ hổng bảo mật trong đó đáng chú ý các lỗ hổng bảo mật sau:

- Lỗ hổng bảo mật CVE-2022-26809 trong RPC Runtime Library cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao trên hệ thống bị ảnh hưởng.

- 02 lỗ hổng bảo mật CVE-2022-24491, CVE-2022-24497 trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao.

- Lỗ hổng bảo mật CVE-2022-26815 trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-26904 trong Windows User Profile Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, lỗ hổng này đã có mã khai thác công khai trên Internet.

- Lỗ hổng bảo mật CVE-2022-26919 trong Windows LDAP cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-24521 trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

Để đảm bảo an toàn thông tin cho hệ thống thông tin dùng chung của tỉnh và của các cơ quan, đơn vị trên địa bàn tỉnh, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Giáo dục và Đào tạo đề nghị đơn vị, trường học chỉ đạo bộ phận chuyên môn thực hiện rà soát, khắc phục các 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 508/CATTTNCSC 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 Quý cơ quan 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.

Sở Giáo dục và Đào tạo đề nghị đơn vị, trường học quan tâm chỉ đạo và phối hợp tổ chức thực hiện./.

Nơi nhận:
- Như trên;
- Ban Giám đốc;
- Các phòng thuộc Sở;
- Lưu: VT, VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XH CHỦ NGHĨA VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH HƯNG YÊN

Đỗ Tiến Hùng