SỞ Y TẾ THANH HÓA **TTYT THIỆU HÓA**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do – Hạnh phúc**
Số: 53/CV-TTYT V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microft công bố tháng 5/2023	*Thiệu Hóa, ngày 08 tháng 6 năm 2023*

Kính gửi: Các khoa, phòng, trạm y tế các xã, thị trấn

Thực hiện công văn số 114/TTCNTT&TT-QTHT về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microft công bố tháng 5/2023.

Căn cứ Công văn số 729/CATTT-NCSC ngày 15/5/2023 về việc cảnh lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 05/2023 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Theo đó, ngày 09/05/2023, Microsoft đã phát hành danh sách bản vá tháng 05 với 38 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng bảo mật CVE-2023-24955 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật CVE-2023-29336, CVE-2023-24902 trong Win32k 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-2023-29325 trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật CVE-2023-24941 trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2023-24932 trong Secure Boot cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đã được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật CVE-2023-29344 trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2023-24953 trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

(Thông tin chi tiết các lỗ hổng bảo mật có tại Phụ lục kèm theo.)

Để tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại các hệ thống thông tin của các đơn vị, Giám đốc Trung tâm Y tế Thiệu Hóa đề nghị các khoa, phòng, trạm y tế các xã, thị trấn thực hiện những nội dung sau:

1. Kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật được công bố trên. Thực hiện cập nhật bản vá bảo mật đối với các lỗ hổng này kịp thời để tránh nguy cơ bị tấn công. Hướng dẫn kỹ thuật cách thức thực hiện chi tiết đối với lỗ hổng bảo mật tại địa chỉ: https://attt.thanhhoa. gov.vn

2. Tăng cường giám sát hoạt động các hệ thống thông tin và sẵn sàng phương án xử lý sự cố 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 quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ với Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa *(cơ quan thường trực của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh)* để phối hợp hỗ trợ, xử lý. Điện thoại: (0237)3718.699, Thư điện tử: ungcuusuco@thanhhoa.gov. Vn.

Nhận được công văn này đề nghị các khoa, phòng, trạm y tế các xã, thị trấn triển khai thực hiện nghiêm túc.

Nơi nhận:
- Như trên;
- Lưu VT, HCTH

GIÁM ĐỐC

SỞ Y TẾ THANH HÓA
TRUNG TÂM Y TẾ HUYỆN THIỆU HÓA

Lê Lương Khang