ỦY BAN NHÂN DÂN HUYỆN ĐÌNH LẬP	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 977/UBND-VHTT V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2024.	*Đình Lập, ngày 20 tháng 5 năm 2024*

Kính gửi
- Các cơ quan, đơn vị sự nghiệp trực thuộc UBND huyện;
- Uỷ ban MTTQ và các tổ chức chính trị - xã hội huyện;
- Các doanh nghiệp Viễn thông, Ngân hàng trên địa bàn;
- UBND các xã, thị trấn;

Căn cứ Công văn số 1117/STTTT-TTCNS ngày 17/5/2024 của Sở Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2024;

Tại Công văn số 884/CATTT-NCSC ngày 16/5/2024 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2024. Theo đó, ngày 14/5/2024, Microsoft đã phát hành danh sách bản vá với 59 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng an toàn thông tin CVE-2024-30040 trong Windows MSHTML Platform cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin CVE-2024-30044 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- 03 lỗ hổng an toàn thông tin CVE-2024-30051, CVE-2024-30032, CVE-2024-30035 trong Windows DWM Core Library cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin CVE-2024-30042 trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin CVE-2024-30033 trong Windows Search Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng an toàn thông tin CVE-2024-30043 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công XXE.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị và góp phần bảo đảm an toàn cho không gian mạng Việt Nam, UBND huyện đề nghị các cơ quan, đơn vị 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 *(hướng dẫn chi tiết tham khảo tại phụ lục đính kèm trên hệ thống Văn phòng điện tử Ioffice)*.

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 quá trình thực hiện nếu có khó khăn, vướng mắc đề nghị liên hệ với Trung tâm Công nghệ số thuộc Sở Thông tin và Truyền thông, số điện thoại **02053.818.657** hoặc trên địa bàn huyện liên hệ Đồng chí: Bế Tiến Vận, chuyên viên Văn phòng HĐND và UBND, số điện thoại: **0911.110.404** để được hỗ trợ./.

UBND huyện Đình Lập trân trọng đề nghị các cơ quan, đơn vị phối hợp triển khai thực hiện./.

Nơi nhận:
- Như trên ;
- Sở Thông tin và Truyền thông ;
- Thường trực Huyện ủy (b/c);
- Thường trực HĐND huyện (b/c);
- Chủ tịch, các PCT UBND huyện;
- Trang Thông tin điện tử huyện;
- Lưu: VT.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Tô Thị Hiến