UỶ BAN NHÂN DÂN **XÃ HÀNH TÍN ĐÔNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số 156/UBND *V/v cảnh báo lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2024*	*Hành Tín Đông, ngày 23 tháng 8 năm 2024*

Kính gửi:

- Các cơ quan, đơn vị; Hội, đoàn thể xã;
- Công an xã;
- CBCC và người hoạt động không chuyên trách xã;

Theo cảnh báo của Sở Thông tin và Truyền thông tại Công văn số 1887/STTTT-BCVT&CNTT ngày 19/8/2024 về lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2024, Thực hiện Công văn số 2096/UBND ngày 23/8/2024 của UBND huyện Nghĩa Hành V/v cảnh báo lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2024, Ủy ban nhân dân xã yêu cầu lãnh đạo các cơ quan, đơn vị và toàn thể cán bộ, công chức cơ quan thực hiện một số biện pháp sau để hạn chế các rủi ro về nguy cơ mất an toàn thông tin, cụ thể:

1. Kiểm tra, rà soát máy chủ, máy trạm có sử dụng hệ điều hành Windows để phát hiện và xử lý kịp thời các máy chủ có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật sau:

(1) Lỗ hổng an toàn thông tin CVE-2024-38063 trong Windows TCP/IP cho phép đối tượng tấn công thực thi mã từ xa.

(2) Lỗ hổng an toàn thông tin CVE-2024-38199 trong Windows Line Printer Daemon (LPD) Service cho phép đối tượng tấn công thực thi mã từ xa. Thông tin chi tiết về lỗ hổng đã được công bố công khai.

(3) Lỗ hổng an toàn thông tin CVE-2024-38189 trong Microsoft Project cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế.

(4) 02 lỗ hổng an toàn thông tin CVE-2024-38218, CVE-2024-38219 trong Microsoft Edge cho phép đối tượng tấn công thực thi mã từ xa.

(5) Lỗ hổng an toàn thông tin CVE-2024-38193 trong Windows Ancillary Function Driver for WinSock cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

(6) Lỗ hổng an toàn thông tin CVE-2024-38107 trong Windows Power Dependency Coordinator cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

(Tham khảo thông tin lỗ hổng và cách khắc phục tại Phụ lục Thông tin về lỗ hổng bảo mật kèm theo Công văn này)

2. Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông báo về UBND xã (qua bộ phận VHXH xã) để tổng hợp báo cáo Phòng Văn hóa thông tin huyện, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi có các biện pháp hỗ trợ, xử lý kịp thời.

Yêu cầu lãnh đạo các cơ quan, đơn vị, cán bộ công chức và người hoạt động không chuyên trách xã quan tâm chỉ đạo thực hiện./.

Nơi nhận:
- Như trên;
- TT. Đảng uỷ xã;
- CT, các PCT UBND xã;
- Lưu VT.

CHỦ TỊCH

Trịnh Bê