ỦY BAN NHÂN DÂN **XÃ CẨM CHÂU**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc Lập - Tự do - Hạnh phúc**
Số:124 /UBND-VH V/v cảnh báo các lỗ hổng bảo mật mới mức độ cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2022	*Cẩm Châu, ngày 04 tháng5 năm 2022*

Kính gửi: - Các ngành, đoàn thể, cán bộ công chức UBND xã,
- Các cơ quan trên địa bàn xã.

Thực hiên công văn số1001/UBND-VHTT ngày 25/04/2022 của UBND huyện Cẩm Thủy về việc cảnh báo các lỗ hổng bảo mật mới mức độ cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2022.

Qua phân tích và đánh giá từ 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 công bố tháng 4/2022. Theo đó, ngày 12/4/2022, hãng Microsoft đã phát hành danh sách bản vá tháng 4 với 128 lỗ hổng bảo mật trong các sản phẩm của mình. Trong đó, bao gồm các lỗ hổng bảo mật có mức ảnh hưởng nghiêm trọng (CVE-2022-26809, CVE-2022-24491, CVE-2022- 24497) và cao (CVE-2022-26815, CVE-2022-26904, CVE-2022-26919, CVE2022-24521).

Theo đánh giá, nếu khai thác thành công các lỗ hổng này cho phép đối tượng tấn công nâng cao đặc quyền từ xa trên hệ thống mục tiêu, từ đó có thể khai thác chiếm quyền điều khiển toàn bộ hệ thống. Trong đó, một số lỗ hổng đã có mã khai thác được đăng tải công khai trên Internet (*Chi tiết các lỗ hổng tại Phụ lục kèm theo).*

UBND xã đề nghị các ngành, đoàn thể, cán bộ, công chức xã và các cơ quan trên địa bàn xã thực hiện tốt một số nội dung sau:

1. Kiểm tra, rà soát và xác định các máy tính, máy chủ đang cài đặt các phần mềm, ứng dụng có khả năng bị ảnh hưởng bởi các lỗ hổng trên để có phương án xử lý, khắc phục lỗ hổng. Cập nhật phiên bản mới nhất theo khuyến nghị của hãng sản xuất để khắc phục các nguy cơ mất an toàn thông tin. Đối với các thiết bị đang sử

dụng các phiên bản của hệ điều hành Windows chưa có bản vá bảo mật, chưa được cài đặt phần mềm phòng chống mã độc tập trung của tỉnh cần thực hiện biện pháp khắc phục thay thế để giảm thiểu nguy cơ tấn công. Hướng dẫn kỹ thuật cách thức thực hiện chi tiết đối với từng lỗ hổng bảo mật tại địa chỉ: https://attt.thanhhoa.gov.vn

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 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 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

UBND xã đề nghị các ngành, đoàn thể, cán bộ, công chức xã và các cơ quan trên địa bàn xã nghiêm túc triển khai, thực hiện./.

Nơi nhận:
- Như trên;
- TT Đảng ủy, HĐND; (Để báo cáo)
- Chủ tịch, Phó Chủ tịch UBND;
- Lưu: VT.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Phạm Thị Khanh