ỦY BAN NHÂN DÂN **HUYỆN TRIỆU SƠN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 4046 /UBND-VHTT V/v dự báo sớm nguy cơ tấn công mạng trên diện rộng.	*Triệu Sơn, ngày 07 tháng 7 năm 2021*

Kính gửi:
- Văn phòng HĐND và UBND huyện;
- UBND các xã, thị trấn;
- Các cơ quan, đơn vị sự nghiệp trên địa bàn huyện.

Thực hiện Công văn số 1392/STTT-CNTT ngày 02/7/2021 của Sở Thông tin và Truyền thông tỉnh về việc dự báo sớm nguy cơ tấn công mạng trên diện rộng. Theo đó, thời gian qua hãng Microsoft có công bố thông tin liên quan tới lỗ hổng bảo mật (CVE-2021-1675) được đánh giá có mức độ nguy hiểm cao (7.8/10) ảnh hưởng đến hầu hết các phiên bản của hệ điều hành Windows bao gồm: Windows 10/8.1/7, Windows Server 2019/2016/2012/2008. Lỗ hổng này cho phép đối tượng tấn công leo thang đặc quyền từ tài khoản người dùng thông thường có rất ít quyền. Qua phân tích và đánh giá từ Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, Bộ Thông tin và Truyền thông mặc dù Microsoft đã phát hành bản vá cho lỗ hổng bảo mật nói trên vào ngày 08/6/2021. Tuy nhiên, lỗ hổng bảo mật (CVE-2021-1675) có mức độ nguy hiểm cao hơn thực tế được công bố. Lỗ hổng này không chỉ đơn giản là khai thác được khi có quyền truy cập trực tiếp vào máy tính/máy chủ cài đặt phiên bản hệ điều hành Windows bị ảnh hưởng, mà còn có thể tấn công thông qua một máy tính trong mạng. Trên cơ sở đó và thực tế triển khai công tác giám sát an toàn thông tin những năm qua, Trung tâm NCSC dự báo sớm lỗ hổng này hoàn toàn có thể được tận dụng để tiến hành các chiến dịch tấn công có chủ đích APT lớn trên quy mô rộng trong thời gian ngắn sắp tới vào không gian mạng Việt Nam.

Để tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại các hệ thống thông tin của các cơ quan, đơn vị trên địa bàn huyện do hình thức tấn công trên có thể xảy ra, UBND huyện đề nghị các cơ quan, đơn vị chỉ đạo các bộ phận, cá nhân thực hiện những nội dung sau:

1. Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo khuyến nghị của Microsoft. Hướng dẫn kỹ thuật cách thức thực hiện tại địa chỉ: https://attt.thanhhoa.gov.vn

2. Tăng cường theo dõi giám sát hệ thống thông tin tại cơ quan, đơn vị mình quản lý; đồng thời thường xuyên theo dõi, cập nhật tình hình về lỗ hổng trên thông qua kênh cảnh báo của các cơ quan chức năng và sẵn sàng, chủ động phương án xử lý khi phát hiện có dấu hiệu bị khai thác, 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;

UBND huyện đề nghị các cơ quan, đơn vị nghiêm túc thực hiện./.

Nơi nhận:
- Như trên;
- Lưu: VT, VHTT.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Lê Quang Trung