ỦY BAN NHÂN DÂN **HUYỆN TRIỆU SƠN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 4811 /UBND-VHTT V/v cảnh báo các lỗ hổng bảo mật mới ảnh hưởng đến hệ điều hành Windows 10, Windows Server và phần mềm Oracle WebLogic Server.	*Triệu Sơn, ngày 26 tháng 8 năm 2021*

Kính gửi:
- UBND các xã, thị trấn;
- VP UBND huyện, VP Huyện ủy;
- Các phòng, ban, ngành, đơn vị sự nghiệp liên quan.

Thực hiện Công văn số 1668/STTTT-CNTT ngày 10/8/2021 của Sở Thông tin và Truyền thông về việc cảnh báo các lỗ hổng bảo mật mới ảnh hưởng đến hệ điều hành Windows 10, Windows Server và phần mềm Oracle WebLogic Server;

Trong thời gian gần đây, Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã ghi nhận các điểm yếu, lỗ hổng bảo mật mới trên các phần mềm, ứng dụng đang được sử dụng rộng rãi trong các hệ thống thông tin của các cơ quan, tổ chức. Trong đó, có những lỗ hổng bảo mật mức cao và nghiêm trọng có thể bị khai thác, sử dụng để tấn công có chủ đích trong diện rộng (Có phụ lục kèm theo công văn 1668/STTTT-CNTT), cụ thể như sau:

- Ngày 20/7/2021, hãng Microsoft đã công bố thông tin về lỗ hổng bảo mật mới (CVE-2021-36934) ảnh hưởng đến hệ điều hành Windows 10 phiên bản 1809/1909/2004/21H1/20H2, Windows Server 2019/20H2. Theo đánh giá, nếu khai thác thành công lỗ hổng này cho phép đối tượng tấn công nâng cao đặc quyền trên hệ thống mục tiêu, từ đó có thể chiếm quyền điều khiển toàn bộ hệ thống. Đặc biệt tại thời điểm hiện nay, lỗ hổng bảo mật chưa có bản vá để cập nhật, trong khi đó trên mạng Internet đã xuất hiện mã khai thác lỗ hổng. Bên cạnh đó, hệ điều hành Windows 10 và Windows Server được sử dụng khá phổ biến hiện nay nên lỗ hổng bảo mật này sẽ có ảnh hưởng tương đối rộng và có thể trở thành mục tiêu hướng đến của các đối tượng tấn công trong thời gian tới.

- Ngày 20/7/2021, hãng Oracle đã công bố 342 bản vá trong bản phát hành các bản vá quan trọng tháng 7/2021 cho các điểm yếu, lỗ hổng có mức ảnh hưởng cao và nghiêm trọng. Nổi bật là 06 lỗ hổng bảo mật (CVE-2021-2394, CVE-2021- 2397, CVE-2021-2382, CVE-2021-2378, CVE-2021-2376, CVE-2021-2403) trong sản phẩm Oracle WebLogic Server. Trong đó 03 lỗ hổng bảo mật (CVE2021-2394, CVE-2021-2397, CVE-2021-2382) có mức ảnh hưởng nghiêm trọng, cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực. Các sản phẩm này của Oracle đều được sử dụng phổ biến trong các hệ thống thông tin cơ quan, tổ chức và doanh nghiệp. Theo đánh giá sơ bộ, những lỗ hổng này sẽ sớm có mã khai thác công khai trên Internet. Điều này có thể dẫn đến nguy cơ tấn công mạng trên diện rộng trong thời gian tới. 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, tổ chức và doanh nghiệp do các 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 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, 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 tại địa chỉ: https://attt.thanhhoa.gov.vn

2. Tăng cường theo dõi giám sát hệ thống đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và sẵn sàng 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./.

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

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Lê Quang Trung