UỶ BAN NHÂN DÂN **HUYỆN SƠN DƯƠNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc Lập – Tự do – Hạnh Phúc**
Số: 2352 /UBND-CNTT V/v ngăn chặn nguy cơ tấn công vào các cơ quan, tổ chức qua lỗ hổng Zerologon	*Sơn Dương, ngày 21 tháng 9 năm 2020*

Kính gửi:

-Các ban Đảng, Văn phòng Huyện ủy;
-Ủy ban MTTQ và các Tổ chức Chính trị - xã hội huyện;
- Các cơ quan, đơn vị thuộc huyện;
- UBND các xã, thị trấn.

Theo đề nghị của Sở Thông tin và Truyền thông tại Văn bản số 617/STTTT-CNTT ngày 17/9/2020 về nguy cơ tấn công vào các cơ quan, tổ chức qua lỗ hổng Zerologon, cụ thể như sau:

1. Sơ lược về lỗ hổng Zerologon

Ngày 11/8/2020 Microsoft đã công bố lỗ hổng CVE-2020-1472 (còn được gọi là Zerologon) trên các máy chủ Domain Controller cho phép đối tượng tấn công thực hiện tấn công leo thang để chiếm quyền quản trị. Domain Controller là máy chủ đóng vai trò trung tâm trong hệ thống mạng triển khai theo mô hình quản lý tập chung, dùng để xác thực và quản lý các máy trạm khác. Khi tấn công được vào máy chủ này, thì đối tượng tấn công xem như kiểm soát toàn bộ hệ thống thông tin của tổ chức.

Theo đánh giá sơ bộ, lỗ hổng này có thể ảnh hưởng đến nhiều cơ quan, tổ chức ở Việt Nam, đầu tháng 9/2020 qua công tác theo dõi, giám sát an toàn thông tin, Trung tâm Giám sát an toàn không gian mạng Quốc gia, Cục an toàn thông tin phát hiện có một số mã khai thác công khai trên Internet. Những mã khai thác này có thể sử dụng để tấn công vào máy chủ Domain Controller qua đó kiểm soát hệ thống thông tin của các cơ quan tổ chức trong các chiến dịch tấn công nguy hiểm. Trong khi đó việc phát hành bản vá đầy đủ cho lỗ hổng Microsoft dự kiến đến Quý I năm 2021 mới hoàn thành.

2. Ủy ban nhân dân huyện đề nghị các cơ quan, đơn vị thuộc huyện, UBND các xã, thị trấn triển khai một số khuyến nghị sau:

- Tổ chức thực hiện rà soát, cập nhật, cài đặt phần mềm diệt virus có bản quyền cho các máy chủ, máy trạm (*bao gồm các máy tính cán bộ nhân viên làm việc*) của các cơ quan, đơn vị mình.

- Tăng cường kiểm tra, giám sát và sẵn sàng có phương án ngăn chặn, sử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng qua việc tận dụng lỗ

hổng để thực hiện cài một số mã khai thác (*mã độc*) này sử dụng các chiến dịch tấn công APT nguy hiểm chiếm quyền quản trị.

- Trong trường hợp cần sự hướng dẫn, kiểm tra chi tiết về lỗ hổng, Các cơ quan, đơn vị, UBND các xã, thị trấn có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng Quốc gia (NCSC), số điện thoại: 0243209616, thư điện tử: *ais@mic.gov.vn.*

Ủy ban nhân dân huyện yêu cầu các cơ quan, đơn vị, thuộc huyện, Uỷ ban nhân các xã, thị trấn nghiêm túc triển khai thực hiện./.

(Có phụ lục Thông tin về lỗ hổng và hướng dẫn vá lỗi gửi kèm)

Nơi nhận:
- Như trên (T/hiện);
- CT, Các PCT UBND huyện(C/đạo);
- Chánh, Các PVPTH HĐND&UBND huyện;
- Các chuyên viên;
- Lưu: VT. (Th.)

TL.CHỦ TỊCH
KT. CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG

Nguyễn Công Thành