

UBND TỈNH KHÁNH HÒA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1875/STTTT-CNTT

V/v cảnh báo lỗ hổng bảo mật mới
ảnh hưởng đến hệ điều hành Windows 10
và Windows Server

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Khánh Hòa, ngày 30 tháng 7 năm 2021

Kính gửi:

- Các cơ quan Đảng, Mặt trận, đoàn thể tỉnh;
- Các sở, ban, ngành;
- UBND các huyện, thị xã, thành phố;
- Các đơn vị sự nghiệp trực thuộc UBND tỉnh.

Sở Thông tin và Truyền thông nhận được Công văn số 984/CATTT-NCSC ngày 23/7/2021 của Cục An toàn thông tin (Bộ Thông tin và Truyền thông) về việc lỗ hổng bảo mật mới ảnh hưởng đến hệ điều hành Windows 10 và Windows Server.

Theo nội dung văn bản nêu trên, ngày 20/7/2021, 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. 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.

Theo đánh giá sơ bộ của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), 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. Đặc biệt tại thời điểm này, lỗ hổng bảo mật chưa có bản vá đồng thời lại có mã khai thác công khai trên Internet. Do vậy, việc khai thác lỗ hổng trở nên dễ dàng hơn dẫn đến gia tăng các nguy cơ tấn công mạng.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị, địa phương, Sở Thông tin và Truyền thông đề nghị Quý cơ quan, đơn vị, địa phương thực hiện các nội dung sau:

1. Kiểm tra, rà soát và xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Tại thời điểm này chưa có bản vá bảo mật cho các máy bị ảnh hưởng, Quý cơ quan, đơn vị, địa phương cần thực hiện biện pháp khắc phục thay thế để giảm thiểu nguy cơ tấn công theo hướng dẫn kèm theo Công văn số 913/CATTT-NCSC (gửi kèm Công văn này)

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.

3. Khẩn trương thông báo nội dung văn bản này đến tất cả các cơ quan, đơn vị trực thuộc để tổ chức triển khai thực hiện.

4. Gửi kết quả thực hiện về Sở Thông tin và Truyền thông qua phần mềm E-Office hoặc thư điện tử: cntt.stttt@khanhhoa.gov.vn trước ngày 15/8/2021.

Quá trình thực hiện nếu có vướng mắc, đề nghị Quý cơ quan, đơn vị, địa phương liên hệ đầu mối thường trực Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (điện thoại: 0258.3563533 - thư điện tử: cntt.stttt@khanhhoa.gov.vn) để được hướng dẫn, hỗ trợ.

Sở Thông tin và Truyền thông thông báo và đề nghị Quý , đơn vị, địa phương quan tâm thực hiện.

Trân trọng./.

Nơi nhận:

- Như trên (VBĐT);
- UBND tỉnh (VBĐT, để b/c);
- Các phòng, đơn vị thuộc Sở (VBĐT, để t/h);
- Lưu: VT, CNTT (V,02).

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Nguyễn Tấn Trung