UBND TỈNH KHÁNH HÒA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1562/STTTT-CNTT

V/v cảnh báo lỗ hổng bảo mật trong BIOS của máy tính, thiết bị Dell

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

Khánh Hòa, ngày 30 tháng 6 năm 2021

KHẨN

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 806/CATTT-NCSC ngày 29/6/2021 của Cục An toàn thông tin (Bộ Thông tin và Truyền thông) về việc 04 lỗ hổng mới trong BIOS của máy tính, thiết bị Dell.

Theo nội dung Công văn số 806/CATTT-NCSC, ngày 24/6/2021, qua công tác giám sát trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) thuộc Cục An toàn thông tin đã ghi nhận **04** điểm yếu, lỗ hổng bảo mật mới **(CVE-2021-21571, CVE-2021-21572, CVE-2021-21573, CVE-021-21574)** trong tính năng BIOSConnect và HTTPS Boot (tính năng, công cụ có sẵn trên hầu hết các máy tính, thiết bị của hãng Dell để hỗ trợ việc cập nhật firmware và khôi phục hệ điều hành từ xa) trên BIOS của các máy tính, thiết bị hãng Dell.

Theo đánh giá, đây là những lỗ hổng có phạm vi ảnh hưởng tương đối lớn, đến khoảng 30 triệu thiết bị tương ứng với 129 dòng máy tính xách tay, máy tính bảng và máy tính bàn. Đặc biệt, 04 lỗ hổng này có thể kết hợp với nhau trong các chiến dịch tấn công có chủ đích để tấn công, kiểm soát máy tính, thiết bị của người dùng, từ đó tấn công sâu hơn vào các hệ thống thông tin quan trọng khác.

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 máy tính, thiết bị có khả năng bị ảnh hưởng bởi các lỗ hổng nêu trên để có phương án xử lý, khắc phục kịp thời; cập nhật bản vá tương ứng theo phát hành của hãng. Trong trường hợp chưa có bản vá cần có phương án để ngăn chặn việc khai thác lỗ hổng, đồng thời theo dõi thường xuyên thông tin về lỗ hổng để cập nhật ngay khi có bản vá (thông tin về lỗ hổng và hướng dẫn chi tiết tại Phụ lục kèm theo Công văn số 806/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.

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 15/7/2021***.

Quá trình thực hiện nếu có vướng mắc, đề nghị Quý cơ quan 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 cơ quan, đơn vị, địa phương quan tâm thực hiện.

Trân trọng./.

Nơi nhận:
- Như trên (VBĐT);
- UBND tỉnh (VBĐT, để b/c);
- Lưu: VT, CNTT (V,02).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH KHÁNH HÒA

Nguyễn Tấn Trung