

**ỦY BAN NHÂN DÂN  
HUYỆN HÀ QUẢNG**

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

Số: /UBND-VHTT

*Hà Quảng, ngày tháng 7 năm 2021*

V/v cảnh báo 04 lỗ hổng bảo mật trong BIOS của máy tính, thiết bị Dell

Kính gửi:

- Các cơ quan, ban, ngành, đoàn thể huyện;
  - UBND các xã, thị trấn.
- (gọi chung là các cơ quan, đơn vị)

Thực hiện Văn bản số 97/TTCNTTTT- KTCGCN ngày 02 tháng 7 năm 2021 của Trung tâm Công nghệ thông tin và Truyền thông tỉnh Cao Bằng Về việc cảnh báo 04 lỗ hổng bảo mật trong BIOS của máy tính, thiết bị Dell.

Ủy ban nhân dân huyện đề nghị các cơ quan, đơn vị phối hợp chỉ đạo triển khai thực hiện một số nội dung sau:

Thực hiện chức năng, nhiệm vụ được giao, qua hoạt động điều phối, hợp tác và chia sẻ thông tin của Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia, Ủy ban nhân dân huyện nhận được cảnh báo tại Công văn số 806/CATTT-NCSC ngày 29/06/2021 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, bao gồm các lỗ hổng có mã **CVE-2021-21571, CVE-2021- 21572, CVE-2021-21573, CVE-2021-21574** 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. 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.

*Ghi chú: Thông tin chi tiết điểm yếu, lỗ hổng và hướng dẫn khắc phục có tại phụ lục kèm theo Công văn số 806/CATTT-NCSC ngày 29/06/2021 của Cục An toàn thông tin (có công văn gửi kèm).*

Nhằm đảm bảo an toàn thông tin cho hệ thống của quý đơn vị, Ủy ban nhân dân huyện đề nghị các cơ quan, đơn vị thực hiện một số nội dung sau:

1. Kiểm tra, rà soát máy tính, thiết bị của hãng Dell có khả năng bị ảnh hưởng bởi các lỗ hổng 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.

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 để phát hiện kịp thời các nguy cơ tấn công mạng.

Trong trường hợp cần thiết có thể liên hệ đầu mối ứng cứu sự cố máy tính tỉnh Cao Bằng: Trung tâm Công nghệ thông tin và Truyền thông Cao Bằng, địa chỉ: Số 009, Hoàng Văn Thụ, Hợp Giang, thành phố Cao Bằng, Điện thoại: 02063.955.899. Email: cbitc@caobang.gov.vn.

Ủy ban nhân dân huyện đề nghị các cơ quan, đơn vị phối hợp chỉ đạo triển khai thực hiện./.

***Nơi nhận:***

- Như trên (VB điện tử);
- Chủ tịch, các PCT UBND huyện;
- Lưu: VT, VHTT (Oanh).

**KT. CHỦ TỊCH  
PHÓ CHỦ TỊCH**

**Nguyễn Thị Phương**