ỦY BAN NHÂN DÂN **HUYỆN VĂN GIANG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 560 /UBND-VHTT V/v cảnh báo 04 lỗ hổng trong BIOS của máy tính, thiết bị DELL và lỗ hổng bảo mật mới trong phần mềm WinRAR	*Văn Giang, ngày 13 tháng 7 năm 2021*

Kính gửi:
- Các cơ quan, đơn vị;
- Ủy ban nhân dân các xã, thị trấn.

Căn cứ Công văn số 670/STTTT-BCVTCNTT ngày 02/7/2021 của Sở Thông tin và Truyền thông tỉnh về việc cảnh báo 04 lỗ hổng trong BIOS của máy tính, thiết bị DELL; Công văn số 695/STTTT-BCVTCNTT ngày 08/7/2021 về việc lỗ hổng bảo mật mới trong WinRAR.

Ủy ban nhân dân huyện yêu cầu các cơ quan, đơn vị; UBND các xã, thị trấn triển khai một số nội dung sau:

1. Kiểm tra, rà soát máy tính, thiết bị của hãng DELL tại đơn vị đang sử dụng có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật mới (**CVE-2021-21571, CVE-2021-21572, CVE-2021-21573, CVE-2021-21574**) có 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. 04 lỗ hổng này có thể kết nối 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 vào các hệ thống thông tin quan trọng khác.

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 *(Theo hướng dẫn tại Công văn số 806/CATT-NCSC của Cục An toàn thông tin gửi kèm).*

2. Thực hiện kiểm tra, rà soát máy tính đang sử dụng phần mềm WinRAR có khả năng bị ảnh hưởng bởi lỗ hổng **CVE-2021-35052** (Khai thác thành công lỗ hổng này, đối tượng tấn công có thể thực hiện tấn công vào hàng loạt các máy tính người dùng đang sử dụng WinRAR, từ đó có thể dẫn đến các chiến dịch tấn công có chủ đích trên diện rộng) để có phương án xử lý, khắc phục lỗ hổng. Cập nhật lên phiên bản mới nhất (hiện tại là 6.02) theo phát hành của hãng *(Theo hướng dẫn theo Công văn số 861/CATTT-NCSC của Cục An toàn thông tin gửi kèm).*

3. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

Trong trường hợp cần hỗ trợ, đề nghị liên hệ đầu mối hỗ trợ của Bộ Thông tin và Truyền thông: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, SĐT: 024.3209.1616, thư điện tử: ais@mic.gov.vn hoặc liên hệ Đội ứng cứu sự cố thông tin mạng tỉnh Hưng Yên, SĐT: 02213.867.093, thư điện tử: cntt.stttt@hungyen.gov.vn.

Yêu cầu các cơ quan, đơn vị; UBND các xã, thị trấn tổ chức triển khai thực hiện./.

Nơi nhận:
- Như kính gửi;
- TT Huyện ủy;
- Lãnh đạo UBND huyện;
- Lưu: VT,VHTT.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Ký bởi: Ủy ban Nhân dân huyện Văn Giang
Cơ quan: Tỉnh Hưng Yên
Thời gian ký: 13/07/2021 14:20:39

Nguyễn Thị An