SỞ THÔNG TIN VÀ TRUYỀN THÔNG
CAO BẰNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 153 /TTCNTTTT-KTCGCN

V/v cảnh báo 19 lỗ hổng bảo mật mới trong VMware

Cao Bằng, ngày 24 tháng 9 năm 2021

Kính gửi:

- Văn phòng Tỉnh uỷ;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành, UBND các huyện và thành phố;
- Toà án nhân dân tỉnh, Viện kiểm sát nhân dân tỉnh;
- Cục thuế tỉnh, Cục Hải quan tỉnh, Cục Quản lý thị trường tỉnh, Bảo hiểm xã hội tỉnh.

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, Trung tâm Công nghệ thông tin và Truyền thông Cao Bằng nhận được cảnh báo tại Công văn số 1286/CATTT-NCSC ngày 22/9/2021 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc 19 lỗ hổng bảo mật mới trong VMware.

Các sản phẩm của VMware được sử dụng khá phổ biến trong các cơ quan tổ chức là mục tiêu nhằm đến của các đối tượng tấn công mạng, đặc biệt là các nhóm chuyên thực hiện tấn công APT. 19 lỗ hổng bảo mật ảnh hưởng đến VMware vCenter Server phiên bản 7.0/6.7/6.5 và VMware vClound Foundation phiên bản 4.3.1/3.10.2.2. Trong đó:

- Lỗ hổng bảo mật **(CVE-2021-22005)** có mức ảnh hưởng nghiêm trọng (điểm CVSS:9.8), cho phép đối tượng tấn công không cần xác thực có thể thực thi mã tùy ý.

- 11 lỗ hổng bảo mật **(CVE-2021-21991, CVE-2021-22006, CVE-2021-22011, CVE-2021-22015, CVE-2021-22012, CVE-2021-22013, CVE-2021-22016, CVE-2021-22017, CVE-2021-22014, CVE-2021-22018, CVE-2021-21992)** có mức ảnh hưởng cao, cho phép đối tượng tấn công khai thác dưới nhiều hình thức khác nhau như thu thập thông tin, tấn công leo thang, tấn công từ chối dịch vụ. Trong đó có 07 lỗ hổng bảo mật **(CVE-2021-22006, CVE-2021-22011, CVE-2021-22012, CVE-2021-22013, CVE-2021-22016, CVE-2021-22017, CVE-2021-22018)** có thể khai thác mà không cần xác thực.

(*Thông tin chi tiết điểm yếu, lỗ hổng và hướng dẫn khắc phục có tại phụ lục kèm theo Công văn số 1286/CATTT-NCSC ngày 22/09/2021 của Cục An toàn thông tin được gửi kèm)*

Nhằm đảm bảo an toàn thông tin cho hệ thống của quý đơn vị, Trung tâm Công nghệ thông tin và Truyền thông kính đề nghị quý cơ quan, đơn vị thực hiện một số nội dung sau:

1. Kiểm tra, rà soát, xác minh hệ thống thông tin có khả năng bị ảnh hưởng bởi lỗ hổng trên để có phương án xử lý, khắc phục lỗ hổng. Thực hiện cập nhật bản vá phù hợp với phiên bản sản phẩm VMware đang sử dụng.

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.

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.

Đề nghị quý cơ quan, đơn vị quan tâm triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở TTTT (b/c);
- Phòng BCVT-CNTT;
- Lưu: VT, KTCGCN.

GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH CAO BẰNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Triệu Đình Thăng