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

Số: 113 /TTCNTTTT-KTCGCN

V/v cảnh báo lỗ hổng mới trong SolarWinds Serv-U Manager File Transfer và Serv-U Secure FTP

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

Cao Bằng, ngày 16 tháng 7 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 913/CATTT-NCSC ngày 14/07/2021 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc lỗ hổng mới trong SolarWinds Serv-U Manager File Transfer và Serv-U Secure FTP.

Serv-U Manager File Transfer và Serv-U Secure FTP là 2 phần mềm, ứng dụng được sử dụng trong nhiều hệ thống công nghệ thông tin của các cơ quan, tổ chức để quản lý, kiểm soát việc truyền, chia sẻ tệp tin bên trong và bên ngoài đơn vị. Lỗ hổng bảo mật **(CVE-2021-35211)** trong Serv-U Manager File Transfer và Serv-U Secure FTP, ảnh hưởng đến phiên bản Serv-U v15.2.3 HF1 (phát hành ngày 05/5/2021) và tất cả các phiên bản trước đó. Đối tượng tấn công có thể khai thác lỗ hổng bảo mật này thông qua giao thức SSH, từ đó thực thi mã từ xa với đặc quyền cao hơn trên máy chủ mục tiêu. (*Thông tin chi tiết điểm yếu, lỗ hổng và hướng dẫn khắc phục có tại phụ lục kèm theo Công văn số 913/CATTT-NCSC ngày 14/07/2021 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 máy chủ có cài đặt SolarWinds Serv-U Manager File Transfer và Serv-U Secure FTP để phát hiện và xử lý kịp thời các máy chủ có khả năng bị đối tượng tấn công khai thác thông qua lỗ hổng trên. Nâng cấp phiên bản tương ứng theo phát hành của hãng. Trong trường hợp chưa thể nâng cấp Quý đơn vị có thể áp dụng biện pháp khắc phục để giảm thiểu nguy cơ bị tấn công.

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