BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

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

Số: 913 /CATTT-NCSC
V/v lỗ hổng mới trong SolarWinds Serv-U Manager File Transfer và Serv-U Secure FTP

Hà Nội, ngày 14 tháng 07 năm 2021

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; các Ngân hàng TMCP; các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Ngày 12/7/2021, SolarWinds đã công bố về 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.

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. Theo đánh giá sơ bộ của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), tại Việt Nam có khoảng 700 hệ thống thông tin của các cơ quan tổ chức sử dụng SolarWinds đang được công khai trên Internet, trong đó có rất nhiều hệ thống của tập đoàn, doanh nghiệp và các công ty lớn.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý đơn vị thực hiện:

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 (tham khảo hướng dẫn kèm theo).

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. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cục trưởng;
- Lưu: VT, NCSC.

CỤC TRƯỞNG

Nguyễn Thành Phúc

Phụ lục
Thông tin về lỗ hổng bảo mật
(Kèm theo Công văn số /CATTT-NCSC ngày / /2021 của Cục An toàn thông tin)

1. Thông tin về các lỗ hổng

Mã lỗ hổng: CVE-2021-35211

Mô tả: Lỗ hổng tồn tại trong Serv-U Manager File Transfer và Serv-U Secure FTP. 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.

Sản phẩm bị ảnh hưởng: phiên bản Serv-U v15.2.3 HF1(phát hành ngày 05/05/2021) và các phiên bản trước đó.

2. Hướng dẫn khắc phục

Cách khắc phục tốt nhất là nâng cấp lên phiên bản mới nhất (**hiện tại là Serv-U v15.2.3 HF2**). Dưới đây là danh sách các phiên bản bị ảnh hưởng và hướng dẫn cập nhật tương ứng:

Phiên bản bị ảnh hưởng	Hướng dẫn cập nhật
Serv-U 15.2.3 HF1	Cập nhật phiên bản Serv-U 15.2.3 HF2, có sẵn trong Customer Portal
Serv-U 15.2.3	Cập nhật lần lượt theo thứ tự lên phiên bản Serv-U 15.2.3 HF1 và Serv-U 15.2.3 HF2, có sẵn trong Customer Portal
All Serv-U versions prior to 15.2.3	Cập nhật lần lượt theo thứ tự lên phiên bản Serv-U 15.2.3, Serv-U 15.2.3 HF1, Serv-U 15.2.3 HF2, có sẵn trong Customer Portal

Trong trường hợp chưa thể nâng cấp phiên bản, Quý đơn vị thực hiện biện pháp khắc phục thay thế bằng cách vô hiệu hóa quyền truy cập SSH trên các sản phẩm bị ảnh hưởng nêu trên.

3. Nguồn tham khảo

https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211