BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

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

Số: 193 /TTCNTT-KTHT
V/v lỗ hổng mới trong SolarWinds Serv-U Manager File Transfer và Serv-U Secure FTP

Hà Nội, ngày 19 tháng 07 năm 2021

Kính gửi: Các đơn vị trực thuộc Bộ có hệ thống 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 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 Cục An toàn thông tin – Bộ Thông tin và Truyền thông, 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 bảo đảm an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Công nghệ 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.

Trong trường hợp cần thiết, Quý đơn vị liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
Thông tin lỗ hổng bảo mật
(Kèm theo Công văn số 193 /TTCNTT-KTHT ngày 19 /07 /2021 của Trung tâm Công nghệ 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

DANH SÁCH CÁC ĐƠN VỊ CÓ HỆ THỐNG THÔNG TIN

(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Thanh tra Bộ
2.	Cục Công tác phía Nam
3.	Cục Ứng dụng và phát triển công nghệ
4.	Cục Năng lượng nguyên tử
5.	Cục Thông tin Khoa học và Công nghệ Quốc gia
6.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
7.	Cục An toàn bức xạ và hạt nhân
8.	Cục Sở hữu trí tuệ
9.	Tổng Cục tiêu chuẩn đo lường chất lượng
10.	Ban quản lý khu công nghệ cao Hoà Lạc
11.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
12.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
13.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
14.	Viện Năng lượng nguyên tử Việt Nam
15.	Viện Ứng dụng công nghệ
16.	Viện Đánh giá khoa học và Định giá công nghệ
17.	Viện Khoa học sở hữu trí tuệ
18.	Viện Nghiên cứu và Phát triển Vùng
19.	Văn phòng các Chương trình trọng điểm cấp nhà nước
20.	Văn phòng Công nhận chất lượng
21.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
22.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
23.	Báo Khoa học và Phát triển
24.	Tạp chí Khoa học và Công nghệ Việt Nam
25.	Nhà xuất bản Khoa học và Kỹ thuật
26.	Quỹ Phát triển khoa học và công nghệ quốc gia
27.	Quỹ Đổi mới công nghệ quốc gia
28.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
29.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế