BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

Số: 474 /CNTT-YTĐT

V/v 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

Hà Nội, ngày 21 tháng 07 năm 2021

Kính gửi:

- Vụ, Cục, Tổng cục, Văn phòng Bộ, Thanh tra Bộ;
- Các đơn vị trực thuộc Bộ Y tế;
- Các Sở Y tế.

Cục Công nghệ thông tin nhận được Công văn số 913 /CATTT-NCSC ngày 14/7/2021 của Bộ Thông tin và Truyền thông về việc lỗ hổng mới trong SolarWinds Serv-U Manager File Transfer và Serv-U Secure FTP.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin, Cục Công nghệ thông tin trân trọng đề nghị Quý đơn vị:

1. Kiểm tra, rà soát máy tính, thiết bị có khả năng bị ảnh hưởng bởi các lỗ hổng trên để có phương án xử lý, khắc phục kịp thời. 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 (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 Trung tâm Dữ liệu y tế, Cục Công nghệ thông tin, Bộ Y tế (ThS. Hoàng Đăng Trị, điện thoại: 0987772483; Email: trihd.cntt@moh.gov.vn) để được hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên;
- Cục trưởng (để b/c);
- Trung tâm Dữ liệu y tế (để thực hiện);
- Lưu: VT, CNTT.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ Y TẾ

Phạm Xuân Viết

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số 474 /CNTT-YTĐT ngày 21 /7/2021 của Cục 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.

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.

2. Nguồn tham khảo

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