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: 413 /TTCNTT-KTHT
V/v cảnh báo nguy cơ tấn công vào phần mềm SolarWinds và lỗ hổng bảo mật trong máy chủ Microsoft Exchange

Hà Nội, ngày 31 tháng 12 năm 2020

Kính gửi: Các đơn vị có hệ thống công nghệ thông tin trực thuộc Bộ

Qua công tác theo dõi, giám sát trên không gian mạng, cùng hoạt động hợp tác, chia sẻ thông tin với các tổ chức lớn về an toàn thông tin trong và ngoài nước, Cục An toàn thông tin – Bộ Thông tin và Truyền thông ghi nhận nguy cơ bị tấn công khi sử dụng phần mềm SolarWinds phiên bản SolarWinds Orion 2019.4 đến 2020.2.1 và 06 lỗ hổng bảo mật **(CVE-2020-17117, CVE-2020-17132, CVE-2020-17141, CVE-2020-17142, CVE-2020-17143, CVE-2020-17144)** trong các máy chủ thư điện tử sử dụng Microsoft Exchange (thông tin chi tiết có tại phụ lục kèm theo).

Ứng dụng SolarWinds thường được sử dụng trong các hệ thống thông tin của các cơ quan, tổ chức để giám sát mạng, hệ thống và cơ sở hạ tầng công nghệ thông tin. Theo đánh giá sơ bộ, lỗ hổng này có thể ảnh hưởng đến nhiều cơ quan, tổ chức ở Việt Nam, đặc biệt là cơ quan chính phủ, ngân hàng, tổ chức tài chính, tập đoàn, doanh nghiệp và các công ty lớn, do các đơn vị này đều triển khai mô hình mạng có sử dụng phần mềm SolarWinds để thuận tiện cho việc quản lý.

Các lỗ hổng "**CVE***" nêu trên ảnh hưởng tới hầu hết các phiên bản Microsoft Exchange cho phép đối tượng tấn công chèn và thực thi mã lệnh trái phép từ đó kiểm soát máy chủ thư điện tử và đánh cắp dữ liệu trên hệ thống. Đối tượng tấn công có thể khai thác lỗ hổng khi có một tài khoản thư điện tử thông thường trên hệ thống. Một số lỗ hổng đã có mã khai thác công khai trên Internet **(CVE-2020-17141, CVE-2020-17143, CVE-2020-17144)**, đã được Cục An toàn thông tin kiểm tra và thử nghiệm. Có nhiều nhóm tấn công cũng đang khai thác các lỗ hổng này để tấn công vào các cơ quan, tổ chức.

Nhằm bảo đảm an toàn thông tin mạng cho hệ thống thông tin của Quý Đơn vị, Trung tâm Công nghệ thông tin đề nghị Quý Đơn vị thực hiện:

1. Rà soát các máy chủ có cài đặt phần mềm SolarWinds Orion hoặc Microsoft Exchange để phát hiện và xử lý kịp thời các máy chủ có khả năng đã bị đối tượng tấn công khai thác thông qua lỗ hổng trên.

2. Kiểm tra, rà soát và xác định toàn bộ các máy chủ bị ảnh hưởng. Cập nhật bản vá hoặc khắc phục lỗ hổng theo hướng dẫn của SolarWinds và Microsoft.

3. Tăng cường theo dõi giám sát hệ thống 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 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 biết);
- 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

(Kèm theo Công văn số 413 /TTCNTT-KTHT ngày 31 /12/2020)

I. Lổ hổng phần mềm SolarWinds

1. Thông tin chung:

- Ảnh hưởng: phiên bản SolarWinds Orion 2019.4 đến 2020.2.1

- Đối tượng tấn công cài cắm phần mềm độc hại (backdoor SUNBERST) vào các bản cập nhật phần mềm SolarWinds Orion.

2. Hướng dẫn cập nhật bản vá:

- Vào ngày 15 tháng 12 năm 2020, SolarWinds đã phát hành bản cập nhật **2020.2.1 HF 2**

để giảm thiểu nguy cơ bị tấn công bởi lỗ hổng bảo mật này.

Truy cập tại: https://customerportal.solarwinds.com/

- Nếu chưa thể cập nhật bản vá:

+) Các quản trị viên có thể ngắt kết nối Internet đối với các sản phẩm SolarWinds Orion phiên bản 2019.4 đến 2020.2.1 HF 1 để tránh rủi ro nguy cơ bị tấn công.

+) Giới hạn phạm vi kết nối từ máy chủ SolarWinds đến các thiết bị đầu cuối.

+) Giới hạn các tài khoản có đặc quyền của quản trị viên trên máy chủ SolarWinds.

+) Cân nhắc việc thay đổi mật khẩu cho các tài khoản có quyền truy cập vào các sản phẩm của SolarWinds.

3. Tên miền độc hại liên quan đến backdoor SUNBERST

*.avsvmcloud.com

- Quý Đơn vị nên giám sát hoặc chặn các kết nối liên quan đến tên miền này.

Thông tin tham khảo tại:

- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

- https://www.solarwinds.com/securityadvisory

II. Lỗ hổng phần mềm Microsoft

STT	CVE	Mô tả
1	CVE-2020-17117	- Điểm CVSS: 7.2 (Cao) - Ảnh hưởng: Exchange Server 2013/2016/2019. - Lỗ hổng cho phép đối tượng tấn công chèn và thực thi mã từ xa. - Cập nhật bản vá bảo mật tại: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17117

2	CVE-2020-17132	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Exchange Server 2013/2016/2019. - Lỗ hổng cho phép đối tượng tấn công chèn và thực thi mã từ xa. - Cập nhật bản vá bảo mật tại: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17132
3	CVE-2020-17141	- Điểm CVSS: 8.4 (Cao) - Ảnh hưởng: Exchange Server 2016/2019. - Lỗ hổng cho phép đối tượng tấn công chèn và thực thi mã từ xa. - Đã có mã khai thác công khai trên Internet. - Cập nhật bản vá bảo mật tại: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17141
4	CVE-2020-17142	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Exchange Server 2013/2016/2019. - Lỗ hổng cho phép đối tượng tấn công chèn và thực thi mã từ xa. - Cập nhật bản vá bảo mật tại: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17142
5	CVE-2020-17143	- Điểm CVSS: 8.8 (Nghiêm trọng) - Ảnh hưởng: Exchange Server 2013/2016/2019. - Lỗ hổng cho phép đối tượng tấn công thu thập thông tin. - Đã có mã khai thác công khai trên Internet. - Cập nhật bản vá bảo mật tại: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17143
6	CVE-2020-17144	- Điểm CVSS: 8.4 (Nghiêm trọng) - Ảnh hưởng: Exchange Server 2010. - Lỗ hổng cho phép đối tượng tấn công chèn và thực thi mã từ xa. - Đã có mã khai thác công khai trên Internet. - Cập nhật bản vá bảo mật tại: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17144