SAO Y; Sở Thông tin và Truyền thông; 25/12/2020; 18:06:38 +07:00

UBND THÀNH PHỐ HẢI PHÒNG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 2647 /STTTT-CNTT
V/v nguy cơ tấn công vào phần mềm SolarWinds và cảnh báo lỗ hổng bảo mật trong máy chủ Microsoft Exchange.

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

Hải Phòng, ngày 25 tháng 12 năm 2020

Kính gửi:
- Các Sở, ban, ngành thành phố;
- Các cơ quan Trung ương tổ chức theo ngành dọc;
- Ủy ban nhân dân các quận, huyện;
- Các tổ chức, doanh nghiệp trên địa bàn.

Ngày 21/12/2020, Cục An toàn thông tin có Công văn số 1204/CATTT-NCSC về việc cảnh báo 06 lỗ hổng bảo mật (CVE-2020-17117, CVE-2020-17132, CVE-2020-17141, CVE-2020-17142, CVE-2020-17143, CVE-2020-17144) trong máy chủ Microsoft Exchange và Công văn số 1207/CATTT-NCSC về việc nguy cơ tấn công vào phần mềm SolarWinds phiên bản SolarWinds Orion 2019.4 đến 2020.2.1 *(gửi kèm văn bản)*,

Sở Thông tin và Truyền thông trân trọng đề nghị các cơ quan, đơn vị rà soát hệ thống công nghệ thông tin và thực hiện các biện pháp phát hiện, ngăn chặn nguy cơ gây mất an toàn thông tin do các lỗ hổng nêu trên gây ra tại cơ quan và các đơn vị trực thuộc theo hướng dẫn của Cục An toàn thông tin tại Công văn số 1204/CATTT-NCSC và 1207/CATTT-NCSC.

Sở Thông tin và Truyền thông cử ông Nguyễn Đông Huy (Trưởng Phòng Hạ tầng kỹ thuật và An toàn thông tin - Trung tâm Thông tin và Truyền thông, số điện thoại 098.4462472) là đầu mối phối hợp, trao đổi thông tin.

Trân trọng./.

Nơi nhận:
- Như trên;
- UBNDTP (để b/c);
- Ban 114 (để b/c);
- GĐ, các PGĐ Sở;
- TT TT&TT;
- Cổng TTĐT Sở, Cổng Tin tức TP;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
THÀNH PHỐ HẢI PHÒNG

Lê Văn Kiên

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

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

Số: 1204/CATTT-NCSC
V/v cảnh báo lỗ hổng bảo mật trong máy chủ Microsoft Exchange

Hà Nội, ngày 21 tháng 12 năm 2020

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.

Hệ thống Cảnh báo điểm yếu và rà soát lỗ hổng bảo mật tự động của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin đã ghi nhận 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. Các lỗ hổng này 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 (thông tin chi tiết có tại phụ lục kèm theo).

Đây là các lỗ hổng mới và một số lỗ hổng đã có mã khai thác công khai trên Internet (CVE-2020-17141, CVE-2020-17143, CVE-2020-17144), đã được Trung tâm NCSC 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 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 đề nghị quý đơn vị thực hiện:

1. Rà soát các máy chủ có cài đặt 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 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 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 Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục trưởng (để b/c);
- PCT Nguyễn Khắc Lịch;
- Lưu: VT, NCSC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Khắc Lịch

Phụ lục
Thông tin các lỗ hổng
(Kèm theo Công văn số /CATTT-NCSC ngày / /2020)

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

Ký bởi: Cục An toàn thông tin
Cơ quan: Bộ Thông tin và Truyền thông
Thời gian ký: 21/12/2020 17:56:44

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 1207/CATTT-NCSC
V/v cảnh báo nguy cơ tấn công vào phần mềm SolarWinds

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

Hà Nội, ngày 21 tháng 12 năm 2020

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.

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 ghi nhận nguy cơ tấn công khi sử dụng phần mềm SolarWinds phiên bản SolarWinds Orion 2019.4 đến 2020.2.1.

Đây là ứng dụng thường 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.

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 đề nghị quý đơn vị thực hiện:

1. Rà soát các máy chủ có cài đặt phần mềm SolarWinds Orion 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.

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 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 Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục trưởng (để b/c);
- PCT Nguyễn Khắc Lịch;
- Lưu: VT, NCSC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Khắc Lịch

Phụ lục

Thông tin lỗ hổng

(Kèm theo Công văn số 1207/CATTT-NCSC ngày 21 /12/2020)

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 vừa qua, SolarWinds đã phát hành bản cập nhật **2020.2.1 HF 2** để giảm thiểu nguy cơ 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 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 thêm có 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