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

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