BỘ CÔNG AN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 08 /TB-BCA-A05	*Hà Nội, ngày 12 tháng 3 năm 2021*

THÔNG BÁO
Về hoạt động tấn công mạng khai thác lỗ hổng bảo mật của Microsoft Exchange

Qua công tác bảo vệ an ninh hệ thống mạng thông tin quốc gia, Bộ Công an phát hiện hoạt động tấn công mạng khai thác lỗ hổng bảo mật phần mềm máy chủ thư điện tử Microsoft Exchange, ảnh hưởng đến an ninh mạng, an toàn thông tin của các cơ quan, tổ chức, doanh nghiệp tại nhiều quốc gia trên thế giới, trong đó có Việt Nam, nội dung cụ thể như sau:

1. Theo công bố của Microsoft ngày 02/3/2021, các máy chủ thư điện tử Microsoft Exchange phiên bản 2013, 2016 và 2019 cài đặt trên máy chủ riêng của khách hàng có 04 lỗ hổng bảo mật zero-day ở mức độ đặc biệt nghiêm trọng (mã lỗi CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065). Lợi dụng các mã lỗi này cho phép tin tặc thực thi các lệnh điều khiển từ xa, qua đó cài đặt các loại mã độc cửa hậu để kiểm soát máy chủ, tải xuống thư điện tử của người dùng mà không cần xác thực; mở rộng leo thang tấn công kiểm soát hệ thống mạng...

Qua điều tra hoạt động tấn công mạng, Bộ Công an phát hiện tin tặc đã tấn công hệ thống thư điện tử của một số cơ quan, đơn vị tại Việt Nam thông qua lỗ hổng bảo mật của Microsoft Exchange, đồng thời, mở rộng tấn công kiểm soát toàn bộ hệ thống mạng, đánh cắp nhiều tài liệu (trong đó có cả tài liệu bí mật nhà nước) được trao đổi qua thư điện tử. Mặc dù Microsoft đã phát hành bản cập nhật cho ứng dụng Microsoft Exchange, tuy nhiên, việc cập nhật bản vá bảo mật của Microsoft chỉ khắc phục được lỗ hổng bảo mật đã được công bố nhưng không gỡ bỏ được các chương trình cửa hậu hoặc các mã độc gián điệp khác được cài cắm trong hệ thống mạng. Nếu không xử lý, ngăn chặn kịp thời dẫn đến nguy cơ mất an ninh mạng, an toàn thông tin, lộ, mất tài liệu nội bộ, bí mật nhà nước.

2. Từ tình hình trên, để đảm bảo an ninh mạng, an toàn thông tin và phòng, chống lộ, mất bí mật nhà nước, Bộ Công an đề nghị các bộ, ban, ngành, địa phương chỉ đạo bộ phận chức năng chủ động thực hiện các biện pháp sau:

- Tổ chức kiểm tra, rà soát ứng dụng Microsoft Exchange đang sử dụng, cập nhật đầy đủ bản vá bảo mật cho ứng dụng theo hướng dẫn của hãng Microsoft[1];

- Tăng cường giám sát an ninh mạng, kịp thời phát hiện hoạt động tấn công mạng; rà soát, loại bỏ chương trình cửa hậu, mã độc gián điệp trên máy chủ; phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an trong điều tra, xác minh, xử lý đối tượng thực hiện tấn công mạng;

- Chấp hành nghiêm chỉnh các quy định của pháp luật về bảo vệ bí mật nhà nước; không lưu trữ, truyền đưa tài liệu bí mật nhà nước qua thư điện tử nếu không áp dụng các giải pháp mã hóa cơ yếu;

- Kết quả kiểm tra, rà soát đề nghị trao đổi bằng văn bản gửi về Bộ Công an qua Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao trước ngày 25/3/2021.

Bộ Công an xin thông báo./.

Nơi nhận:
- Đ/c Bộ trưởng Tô Lâm
- Các đồng chí Thứ trưởng

(để báo cáo);

- Văn phòng TW Đảng
- Văn phòng Tổng Bí thư
- Văn phòng Chủ tịch nước
- Văn phòng Quốc hội
- Văn phòng Chính phủ
- Các bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ
- Tỉnh ủy, Thành ủy, UBND các tỉnh, TP trực thuộc TW
- Tòa án nhân dân tối cao
- Viện kiểm sát nhân dân tối cao
- Kiểm toán nhà nước

(để phối hợp);

- Các tập đoàn, tổng công ty: EVN, PVN, VNA, VATM, ACV
- Công an các đơn vị trực thuộc Bộ
- Công an các tỉnh, thành phố trực thuộc TW

(để thực hiện);

- Lưu: VT, A05(P8).

TUQ. BỘ TRƯỞNG
CỤC TRƯỞNG CỤC AN NINH MẠNG VÀ PCTP SỬ DỤNG CÔNG NGHỆ CAO

Trung tướng Nguyễn Minh Chính

[1] Địa chỉ cập nhật bản vá: https://msrc.microsoft.com/update-guide/vulnerability