BỘ CÔNG AN
CÔNG AN TỈNH NGHỆ AN

Số: 1318 /CAT-PA05

V/v phòng ngừa lỗ hổng bảo mật nghiêm trọng trong Microsoft Office

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

Nghệ An, ngày 06 tháng 6 năm 2022

Kính gửi:
- Giám đốc các Sở, ban, ngành cấp tỉnh;
- Chủ tịch UBND các huyện, thành phố, thị xã.

Ngày 30/5/2022, Microsoft cảnh báo lỗ hổng bảo mật nghiêm trọng có tên Follina (CVE-2022-30190, điểm CVSS 7.8/10) tồn tại trên bộ công cụ Microsoft Office[1]. Theo đó, lỗ hổng trên được ghi nhận ảnh hưởng đến các sản phẩm của Microsoft như: Hệ điều hành Windows 7, 8, 10, 11; Windows Server 2008, 2012, 2016, 2019, 2022 và các phiên bản Microsoft Office 2013, 2016, 2019, 2021[2]. Tuy lỗ hổng mới được phát hiện nhưng với cách khai thác đơn giản chỉ bằng cách lừa người dùng mở hoặc xem một tài liệu Word độc hại, tin tặc đã có thể kích hoạt lỗ hổng và thực thi mã từ xa trên thiết bị của nạn nhân như cài đặt chương trình, xem, thay đổi hoặc xóa dữ liệu, đánh cắp thông tin, dữ liệu, tạo tài khoản mới.

Qua theo dõi, hiện Microsoft chưa công bố bản vá lỗ hổng trên; Công an tỉnh chưa ghi nhận hoạt động tấn công, khai thác lỗ hổng trên vào các máy tính thuộc quản lý của cơ quan nhà nước trên địa bàn tỉnh. Tuy nhiên, nhiều khả năng mã khai thác sẽ sớm được các đối tượng tin tặc, tội phạm mạng chia sẻ, rao bán để thực hiện tấn công mạng; nguy cơ ảnh hưởng tới hàng nghìn máy tính và hệ thống thông tin của các cơ quan, tổ chức tại Nghệ An.

Từ tình hình trên, để tăng cường bảo đảm an ninh mạng, an toàn thông tin, phòng ngừa, ngăn chặn hoạt động lợi dụng lỗ hổng bảo mật trên để tấn công mạng và thực hiện nhằm vào các mục đích xấu, Công an tỉnh đề nghị các sở, ban, ngành, UBND các huyện, thành phố, thị xã chỉ đạo bộ phận chuyên trách triển khai một số biện pháp sau:

1. Thực hiện giải pháp tạm thời để vô hiệu hóa giao thức MSDT URL, ngăn việc khởi chạy các liên kết thông qua hệ điều hành

- Chạy **Command Prompt** với quyền **Administrator** (Quản trị viên);

- Sao lưu cấu hình có khóa ms-msdt filename trong Registry, thực hiện lệnh **"reg export HKEY_CLASSES_ROOT\ms-msdt filename";**

---

[1] Microsoft Office là bộ phần mềm các ứng dụng văn phòng hỗ trợ các công việc quản lý nhập dữ liệu, trình bày, thống kê dữ liệu; bao gồm Microsoft Word, Microsoft Excel, Microsoft PowerPoint,...

[2] Tham khảo thêm tại: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

- Thực hiện lệnh **"reg delete HKEY_CLASSES_ROOT\ms-msdt /f"** để xóa cấu hình ms-msdt khỏi thiết bị.

2. Tắt chế độ Preview trong Windows Explorer

Mở **Windows Explorer**, sau đó vào tab **View** rồi chọn **Hide Preview Pane**.

3. Cập nhật phần mềm diệt virus (nếu có); cảnh giác khi tải về bất kỳ file office và kiểm tra kỹ file bằng công cụ Virus Total trước khi mở hoặc sử dụng các phần mềm online Google Docs, Sheet, Slide để xem nội dung file.

4. Khi phát hiện máy tính bị tấn công, khai thác bằng lỗ hổng trên, cần cách ly vật lý khỏi hệ thống thông tin. Thường xuyên theo dõi để cập nhật thông tin về bản vá mới nhất từ Microsoft để xử lý triệt để lỗ hổng trên.

Quá trình thực hiện nếu có khó khăn, vướng mắc kịp thời trao đổi Công an tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao)* để được hướng dẫn./.

Nơi nhận:
- Như trên (để phối hợp);
- Chủ tịch UBND tỉnh;
- PCT Thường trực UBND tỉnh; } (để báo cáo)
- Phòng PV01 (để theo dõi);
- Công an các huyện, thành, thị (để th/hiện);
- Lưu: VTCAT (gốc), PA05 (Đ1).

GIÁM ĐỐC

CÔNG HOÀ X.H.C.N VIỆT NAM
CÔNG AN TỈNH NGHỆ AN

Thiếu tướng Phạm Thế Tùng