BỘ CÔNG AN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 3396 /BCA-A05 V/v lỗ hổng bảo mật Microsoft SharePoint CVE-2025-53770	*Hà Nội, ngày 29 tháng 7 năm 2025*

Kính gửi:

- Các Bộ, Cơ quan ngang Bộ, Cơ quan thuộc Chính phủ;
- Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Tòa án nhân dân tối cao, Viện Kiểm sát nhân dân tối cao, Kiểm toán Nhà nước;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn kinh tế, Tổng Công ty Nhà nước, các Ngân hàng TMCP; các tổ chức tài chính.

Ngày 19/7/2025, Microsoft đã công bố thông tin về lỗ hổng bảo mật nghiêm trọng CVE-2025-53770 trong sản phẩm Microsoft SharePoint On-premises, cho phép đối tượng tấn công thực thi mã từ xa. Sản phẩm này của Microsoft được sử dụng phổ biến trong các hệ thống thông tin cơ quan, tổ chức nhà nước; ngân hàng, tổ chức tài chính, tập đoàn, doanh nghiệp và các công ty lớn. Đặc biệt, lỗ hổng này có thể đã, đang và sẽ được các nhóm tấn công có chủ đích (APT) sử dụng để khai thác diện rộng trong thời gian này. Thông tin cụ thể về lỗ hổng như sau:

- Điểm CVSS: 9.8/10; Mức độ: Rất nghiêm trọng;

- Lỗ hổng khai thác lỗi bỏ qua xác thực được kích hoạt bằng cách đặt header "Referer" thành "/_layouts/SignOut.aspx"". Sau đó được khai thác để kích hoạt thực thi mã từ xa thông qua webshell "/_layouts/15/ToolPane.aspx".

- Lỗ hổng ảnh hưởng đến các phiên bản Microsoft SharePoint Server 2019 và Microsoft SharePoint Enterprise Server 2016. Biện pháp khắc phục lỗ hổng là cập nhật các bản vá hoặc sử dụng các biện pháp giảm thiểu nguy cơ tấn công. Ngày 21/7/2025, Microsoft đã đưa ra các bản vá bảo mật cần thiết (tham khảo trang web của hãng: https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/).

Nhằm đảm bảo an ninh mạng cho hệ thống thông tin của các cơ quan, góp phần bảo đảm an ninh mạng cho không gian mạng Việt Nam, Bộ Công an yêu cầu các cơ quan đơn vị chỉ đạo thực hiện:

1. Kiểm tra, rà soát và xác định máy chủ sử dụng phiên bản SharePoint có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo hướng dẫn của Microsoft.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo kịp thời của các cơ quan chức năng và các tổ chức lớn về an ninh mạng để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Trong trường hợp phát hiện dấu hiệu tấn công mạng khai thác lỗ hổng bảo mật trên, đề nghị các đơn vị liên hệ Trung tâm An ninh mạng quốc gia, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an để báo cáo sự cố và được hướng dẫn hỗ trợ, điện thoại: 0593.505.999, thư điện tử: contact@nca.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Đ/c Bộ trưởng (để báo cáo);
- Lưu: VT, A05.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Thượng tướng Phạm Thế Tùng