UBND THÀNH PHỐ ĐÀ NẴNG
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 555 /SGDĐT-QLCL

V/v khắc phục lỗ hổng bảo mật Microsoft SharePoint CVE 2025-53770

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

Đà Nẵng, ngày 13 tháng 8 năm 2025

Kính gửi:
- Ủy ban nhân dân xã, phường, đặc khu;
- Các trường trực thuộc Sở.

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 điển 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).

Ngày 05/8/2025, Sở Giáo dục và Đào tạo (GDĐT) nhận được Công văn số 549/CATP-PA05 của Công an thành phố về việc nguy cơ lỗ hổng bảo mật Microsoft SharePoint CVE 2025-53770. Nhằm bảo đảm an ninh mạng, khắc phục lỗ hổng bảo mật, Sở GDĐT đề nghị các đơn vị trường học trên địa bàn thành phố thực hiện một số nội dung sau:

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; 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 liên hệ đầu mối của Công an thành phố qua PA05 (đồng chí

Thượng úy Nguyễn Quốc Huy - Cán bộ Đội 2, Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Số điện thoại: 0948.597.555) để trao đổi sự cố và được hướng dẫn hỗ trợ.

Sở GDĐT đề nghị các đơn vị, trường học triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Công an thành phố;
- Giám đốc, Phó Giám đốc;
- Lưu: VT, QLCL.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
THÀNH PHỐ ĐÀ NẴNG

Nguyễn Hoàng Nam