**HƯỚNG DẪN KIỂM TRA, KHẮC PHỤC LỖ HỎNG BẢO MẬT**

**MICROSOFT SHAREPOINT CVE-2025-53770**

(*Ban hành kèm theo công văn số* /CAT*-PA05(Đ4), ngày* / */2025)*

**1. Kiểm tra, rà soát hệ thống SharePoint trong cơ quan, đơn vị**

Xác định các máy chủ SharePoint on-premises (cài đặt nội bộ) dang sử dụng thuộc phiên bản SharePoint Server 2016, SharePoint Server 2019 hoặc SharePoint Subscription Edition (nếu có). Tiến hành kiểm tra dấu hiệu tấn công (dấu hiệu xâm nhập) theo các bước sau:

• Rà soát nhật ký truy cập (IIS log) trên máy chủ SharePoint xem có các yêu cầu HTTP bất thường tới đường dẫn/ layouts/15/ToolPane.aspx?DisplayMode–Edit hay không, đặc biệt là những yêu cầu gửi phương thức POST tới URL trên kèm header “Referer” trỏ đến /\_layouts/SignOut.aspx. Đây là dấu hiệu điển hình của việc khai thác lỗ hổng CVE-2025-53770, cho thấy kẻ tấn công đã giả mạo header để qua mặt cơ chế xác thực và cố gắng tải tập tin độc hại lên hệ thống. Ngoài ra, kiểm tra xem trong log có truy cập đến tệp tin lạ như /\_layouts/15/spinstall0.aspx hay không – nếu có nghĩa là máy chủ đã bị cài webshell và kẻ tấn công dang kiểm soát từ xa.

•Kiểm tra tệp tin cài đặt trên máy chủ: Truy cập vào thư mục cài đặt SharePoint (thư mục LAYOUTS mặc định, ví dụ đường dẫn: C:\Program Files\Common Files\Microsoft Shared Web Server Extensions\16\TEMPLATE LAYOUTS\) và tìm kiếm xem có xuất hiện các tập .aspx bất thường hay không. Đặc biệt chú ý hai tệp: spinstall0.aspx và debug\_dev.js, nếu có thì gần như chắc chắn hệ thống dã bị khai thác (đây là các webshell/tập tin được tạo ra sau khi kẻ tấn công thực thi mã độc trên máy chủ).

• Giám sát tiến trình dịch vụ: Kiểm tra các tiến trình trên máy chủ SharePoint (ví dụ tiến trình w3wp.exe của IIS) xem có hành vi bất thường hay không. Dấu hiệu nghi ngờ bao gồm trường hợp tiến trình w3wp.exe tự động khởi chạy các tiến trình Command Prompt hoặc PowerShell – điều này có thể cho thấy kẻ tấn công dang sử dụng webshell để thực thi lệnh trên máy chủ.

• Rà soát kết nối mạng đáng ngờ: Phân tích log tường lửa, log mạng để phát hiện các kết nối từ máy chủ SharePoint đến những địa chỉ IP bất thường/độc hại trong khoảng thời gian nghi vấn (ví dụ từ ngày 17/7/2025 đến nay). Hiện đã có danh sách một số địa chỉ IP được xác định là máy chủ điều khiển (C2) trong chiến dịch tấn công này, bao gồm: 107.191.58[.]76, 104.238.159|.]149,96.9.125.]147, 139.144.199|.|41,.... Nếu phát hiện kết nối đến các IP nêu trên hoặc IP đáng ngờ khác, cần đặc biệt lưu ý và đưa vào diện nghi vấn cao.

2

Sử dụng công cụ rà quét tự động: Cơ quan, đơn vị có thể sử dụng công cụ kiểm tra lỗ hổng CVE-2025-53770 do chuyên gia ZehprFish phát triển (mã nguồn công khai trên Gitl Iub) nhằm hỗ trợ quá trình rà soát. Công cụ này sẽ gửi các truy vấn POST mô phỏng hành vi tấn công và kiểm tra phản hồi. Nếu máy chủ bị khai thác, công cụ có thể phát hiện dấu hiệu rò rỉ “khóa máy” (machine key) của hệ thống SharePoint, bao gồm các khóa ValidationKey, DecryptionKey – những khóa dùng để mã hóa và xác thực ViewState của ASP.NET. Việc phát hiện phản hồi chứa chuỗi khóa (định dạng phân tách bằng ký tự () là bằng chứng rõ ràng cho thấy máy chủ đã bị xâm nhập và lộ khóa bảo mật. Bên cạnh đó, công cụ còn tự động kiểm tra sự tồn tại của webshell (như file spinstall0.aspx) cùng một số payload độc hại khác, đồng thời nhận diện các chỉ số tấn công (loC) di kèm (chẳng hạn chuỗi mã độc ASP.NET, header HTTP bất thường) và đưa ra cảnh báo mức Critical nếu phát hiện dấu hiệu nguy hiểm. (Lưu ý: Khi sử dụng công cụ cần thực hiện trên một máy tính nội bộ tin cậy, có kết nối đến máy chủ SharePoint, hoặc cấu hình mở cổng phù hợp trên tường lửa để công cụ có thể gửi truy vấn đến máy chủ SharePoint nội bộ).

**2. Cập nhật bản vá và thực hiện biện pháp khắc phục**

Đối với các máy chủ SharePoint xác định có nguy cơ ảnh hưởng, cần tiến hành cập nhật bản vá bảo mật sớm nhất có thể. Cụ thể, áp dụng ngay các bản vá do Microsoft phát hành ngày 21/7/2025 cho SharePoint Server Subscription Edition và SharePoint Server 2019. (Đối với SharePoint 2016, Microsoft dự kiến sẽ sớm cung cấp bản vá tương ứng; các cơ quan, đơn vị cần theo dõi để cập nhật ngay khi có bản vá chính thức). Trường hợp chưa thể cập nhật ngay (hoặc đối với phiên bản chưa có bản vá), thực hiện các biện pháp giảm thiểu sau:

Kích hoạt các tính năng bảo mật bổ trợ: Bật chức năng AMSI (Antimalware Scan Interface) cho máy chủ SharePoint và dảm bảo máy chủ đã cài đặt và kích hoạt phần mềm chống virus (như Microsoft Defender hoặc giải pháp tương đương). Nếu SharePoint chưa kích hoạt được tính năng AMSI, cần hạn chế kết nối Internet của máy chủ (tách máy chủ SharePoint ra khỏi vùng mạng có truy cập internet) để giảm thiểu nguy cơ bị tấn công cho đến khi có bản vá.

• Cô lập và làm sạch hệ thống bị nghi xâm nhập: Nếu qua quá trình kiểm tra phát hiện dấu hiệu hệ thống đã bị khai thác, cần ngay lập tức cô lập máy chủ (ngắt kết nối mạng) để tránh lây lan. Thực hiện quét virus toàn bộ và kiểm tra thủ công để xóa bỏ các webshell, mã độc đã được cài cắm (xóa các file .aspx lạ như spinstall0.aspx, debug\_dev.js đã nêu, gỡ bỏ các dịch vụ, tác vụ bất thường, v.v.). Song song đó, thu thập nhật ký, bằng chứng phục vụ điều tra sự cố sau này.

• Thay đổi thông tin bảo mật quan trọng: Tiến hành đổi các khóa máy (machine key) của SharePoint, đặc biệt là hai khóa ValidationKey và DecryptionKey dùng trong cơ chế ViewState của hệ thống. Việc thay đổi khóa nên thực hiện ngay lập tức (nếu nghi ngờ đã bị lộ) và lặp lại lần nữa sau khi cập nhật bản vá. Sau khi thay đổi khóa, cần khởi động lại dịch vụ IIS trên máy chủ để áp dụng thay đổi. Biện pháp này nhằm phòng ngừa trường hợp kẻ tấn công đã dánh cắp các khóa cũ – nếu chỉ vá lỗi mà không thay khóa, đối tượng có thể vẫn duy trì quyền truy cập trái phép về sau.

• Đổi mật khẩu và kiểm tra tài khoản: Thực hiện đổi mật khẩu toàn bộ các tài khoản dịch vụ đang được SharePoint sử dụng (tài khoản chạy dịch vụ, tài khoản kết nối CSDL, v.v.). Đồng thời rà soát danh sách tài khoản người dùng trong hệ thống Active Directory/SharePoint xem có tài khoản quản trị viên nào bị tạo mới hoặc có dấu hiệu lạm dụng hay không; nếu có, cần vô hiệu hóa hoặc xóa bỏ các tài khoản dáng ngờ ngay.