

Cảnh báo 9 lỗ hổng nguy cơ cao và nghiêm trọng về an toàn thông tin trong các sản phẩm của Microsoft

16:05 18/07/2023

Cục An toàn thông tin (Bộ TT&TT) vừa đưa ra cảnh báo các cơ quan, tổ chức, doanh nghiệp về các lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm của Microsoft.

Từ danh sách bản vá tháng 7/2023 đối với 130 lỗ hổng an toàn thông tin (ATTT) trong các sản phẩm của Microsoft do hãng công bố, các chuyên gia Cục ATTT đã đánh giá và lưu ý các đơn vị chuyên trách về CNTT, ATTT về 9 lỗ hổng ảnh hưởng mức cao và nghiêm trọng.

Đáng chú ý, trong 9 lỗ hổng mới được cảnh báo, có 2 lỗ hổng CVE-2023-33160 và CVE-2023-33134 tồn tại trong phần mềm Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa.



Bộ TT&TT cảnh báo 9 lỗ hổng mới nguy cơ cao và nghiêm trọng về an toàn thông tin

Thời gian vừa qua, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC thuộc Cục ATTT) đã nhiều lần cảnh báo diện rộng về những lỗ hổng ảnh hưởng đến Microsoft SharePoint Server. Điều này cho thấy, Microsoft SharePoint Server vẫn là mục tiêu hàng đầu được các đối tượng tấn công có chủ đích nhắm đến.

Để đảm bảo ATTT cho hệ thống của các cơ quan, tổ chức, Cục ATTT đề nghị các đơn vị rà soát lỗ hổng liên quan đến Microsoft SharePoint Server để phát hiện và có phương án xử lý kịp thời, đồng thời tăng cường giám sát nhằm giảm thiểu nguy cơ bị tấn công thông qua các lỗ hổng này.

Bên cạnh 2 lỗ hổng mới trong Microsoft SharePoint Server, Cục cũng đề nghị các đơn vị đặc biệt lưu ý 7 lỗ hổng bảo mật khác trong các sản phẩm của Microsoft, có thể bị các nhóm tin tặc lợi dụng, khai thác để tấn công vào các hệ thống thông tin tại Việt Nam.

Trong đó có 2 lỗ hổng bảo mật CVE-2023-32057 và CVE-2023-35309 trong Microsoft Message Queuing, cho phép đối tượng tấn công thực thi mã từ xa. Đây là 2 lỗ hổng được đánh giá có mức độ ảnh hưởng nghiêm trọng, với điểm CVSS là 9.8.

Cùng có mức độ ảnh hưởng ở mức cao, với điểm CVSS từ 7.8 đến 8.8, có 5 lỗ hổng gồm CVE-2023-36884 trong Office và Windows, CVE-2023-35311 trong Microsoft Outlook, CVE-2023-36874 trong Windows Error Reporting Service, CVE-2023-32046 trong Windows MSHTML và CVE-2023-32049 trong Windows SmartScreen đều đang bị khai thác trong thực tế.

Cục ATTT khuyến nghị các đơn vị kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng; có biện pháp xử lý kịp thời để tránh nguy cơ bị tấn công. Trong đó, biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật theo hướng dẫn của hãng.

Các cơ quan, tổ chức, doanh nghiệp tăng cường việc 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 của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Tâm An (t/h)