TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Cảnh báo 06 lỗ hổng ảnh hưởng mức cao và nghiêm trọng trong các sản phẩm được Microsoft

10:54 21/10/2023

Trung tâm Giám sát an toàn không gian mạng quốc gia - NCSC thuộc Cục An toàn thông tin, Bộ TT&TT vừa cảnh báo các cơ quan, đơn vị, doanh nghiệp về 06 lỗ hổng ảnh hưởng mức cao và nghiêm trọng trong các sản phẩm được Microsoft công bố tháng 10/2023.



Ảnh minh họa internet.

Cụ thể, trong 06 lỗ hổng an toàn thông tin mới được Cục An toàn thông tin cảnh báo các đơn vị, có lỗ hổng CVE-2023-36778 trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

Trước đó, Trung tâm Giám sát an toàn không gian mạng quốc gia đã nhiều lần phát hành các văn bản cảnh báo diện rộng về những lỗ hổng ảnh hưởng đến hệ thống máy chủ thư điện tử - Microsoft Exchange Server. Qua đó cho thấy, Microsoft Exchange Server vẫn luôn là mục tiêu hàng đầu được các đối tượng tấn công có chủ đích nhắm đến.

Vì vậy, để đảm bảo an toàn thông tin cho hệ thống của các cơ quan, tổ chức, Cục An toàn thông tin, Bộ Thông tin và Truyền thông (TT&TT) đề nghị các cơ quan, tổ chức, doanh nghiệp rà soát lỗ hổng liên quan đến Microsoft Exchange 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.

Cũng trong lần cảnh báo này, Trung tâm Giám sát an toàn không gian mạng quốc gia đề nghị các đơn vị lưu ý 05 lỗ hổng an toàn thông tin khác tồn tại trong sản phẩm của hãng Microsoft, bao gồm lỗ hổng CVE-2023-36563 trong Microsoft WordPad cho phép đối tượng tấn công thực hiện thu thập thông tin mã băm NTLM của người dùng; 02 lỗ hổng CVE-2023-41763 trong Skype for Business và CVE-2023-36434 trong Windows IIS Server đều cho phép đối tượng tấn công thực hiện leo thang đặc quyền; và 02 lỗ hổng CVE-2023-35349, CVE-2023-36697 trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

Các chuyên gia NCSC cũng lưu ý thêm, các lỗ hổng CVE-2023-36563 tồn tại ở sản phẩm Microsoft WordPad, CVE-2023-41763 trong Skype for Business hiện đang bị khai thác trong thực tế.

Để đảm bảo an toàn thông tin cho hệ thống thông tin của đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin vừa có một số khuyến nghị với đơn vị chuyên trách CNTT, an toàn thông tin của các bộ, ngành, địa phương; các tập đoàn, tổng công ty nhà nước và các ngân hàng, tổ chức tài chính.

Cùng với đề nghị kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi 06 lỗ hổng nêu trên hay không, Cục An toàn thông tin hướng dẫn rõ, trường hợp bị ảnh hưởng, các đơn vị cần thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công.

Các cơ quan, tổ chức, doanh nghiệp cũng được đề nghị 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 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.

Hà Trần