TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Cục An toàn thông tin đề nghị các đơn vị rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng

16:03 14/11/2022

Thông tin về các lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 11/2022 vừa được Cục An toàn thông tin, Bộ TT&TT cảnh báo tới đơn vị chuyên trách về CNTT các bộ, ngành, địa phương; các tập đoàn, tổng công ty nhà nước; các ngân hàng nhà nước; các ngân hàng, tổ chức tài chính cùng hệ thống các đơn vị chuyên trách về an toàn thông tin.



Ảnh minh hoạ internet.

Theo Cục An toàn thông tin, trong danh sách bản vá tháng 11 với 64 lỗ hổng bảo mật mới được Microsoft phát hành ngày 8/11 vừa qua, đáng lưu ý là 18 lỗ hổng có mức ảnh hưởng cao và nghiêm trọng.

Trong đó, có 6 lỗ hổng CVE-2022-41082, CVE-2022-41040, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078, CVE-2022-41123 tồn tại trong Microsoft

Exchange Server cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền.

Hai lỗ hổng CVE-2022-41128, CVE-2022-41118 trong Windows Scripting Languages cho phép đối tượng tấn công thực thi mã từ xa. “Các lỗ hổng này đang bị khai thác trong thực tế”, Cục An toàn thông tin cho biết thêm.

Cùng với đó, còn có lỗ hổng CVE-2022-41091 trong Windows Mark of the Web cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. Lỗ hổng CVE-2022-41073 trong Windows Print Spooler cho phép đối tượng thực hiện tấn công nâng cao đặc quyền.

Lỗ hổng CVE-2022-41125 trong Windows CNG Key Insolation Service cho phép đối tượng thực hiện tấn công nâng cao đặc quyền.

Ba lỗ hổng CVE-2022-41044, CVE-2022-41088, CVE-2022-41039 trong Windows Point-to-Point cho phép đối tượng tấn công thực thi mã từ xa.

Với 4 lỗ hổng CVE-2022-41105, CVE-2022-41106, CVE-2022-41063, CVE-2022-41104 trong Microsoft Excel, các lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa, tấn công giả mạo, thực hiện tấn công vượt qua cơ chế bảo mật.

Để đảm bảo an toàn thông tin cho hệ thống thông tin của đơn vị mình, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị các cơ quan, tổ chức, doanh nghiệp kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Trường hợp bị ảnh hưởng, đơn vị cần cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công.

Các cơ quan, tổ chức, doanh nghiệp cũng được yêu cầu 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.

Trường hợp cần thiết, các đơn vị có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin là Trung tâm Giám sát an toàn không gian mạng quốc gia theo số điện thoại 02432091616, và thư điện tử ais@mic.gov.vn.

Hà Trần