

Cảnh báo về các lỗ hổng an toàn thông tin trong các sản phẩm Microsoft

09:27 15/07/2024

Mới đây, Cục An toàn thông tin đã có cảnh báo về các lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố bản vá tháng 7/2024.

Cảnh báo lần này tiếp tục được Cục An toàn thông tin, Bộ Thông tin và Truyền thông (TT&TT) gửi tới đơn vị chuyên trách CNTT, an toàn thông tin của các bộ, ngành và địa phương; các tập đoàn, tổng công ty nhà nước; các Ngân hàng thương mại cổ phần, các tổ chức tài chính.



Ảnh minh họa

Theo cảnh báo, từ 139 lỗ hổng an toàn thông tin tồn tại trong các sản phẩm Microsoft mới được hãng công nghệ này cập nhật bản vá, các chuyên gia Cục An toàn thông tin khuyến nghị các cơ quan, tổ chức và doanh nghiệp trong cả nước đặc biệt lưu ý 10 lỗ hổng có mức ảnh hưởng cao và nghiêm trọng.

Trong số 10 lỗ hổng an toàn thông tin mới được cảnh báo, có 8 lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, bao gồm: Ba lỗ hổng CVE-2024-

38074, CVE-2024-38076 và CVE-2024-38077 tồn tại trong Windows Remote Desktop Licensing Service; lỗ hổng CVE-2024-38060 trong Windows Imaging Component; ba lỗ hổng CVE-2024-38023, CVE-2024-38024, CVE-2024-38094 trong Microsoft SharePoint Server; lỗ hổng CVE-2024-38021 trong Microsoft Office.

Đáng chú ý, có 2 lỗ hổng an toàn thông tin hiện đang bị hacker khai thác trong thực tế, đó là lỗ hổng có mã CVE-2024-38080 tồn tại trong Windows Hyper-V cho phép đối tượng tấn công thực hiện leo thang đặc quyền; lỗ hổng CVE-2024-38112 trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo – Spoofing.

Để đảm bảo an toàn cho hệ thống thông tin của đơn vị, góp phần bảo đảm an toàn không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị các cơ quan, tổ chức, doanh nghiệp trên toàn quốc tiến hành kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi các lỗ hổng an toàn thông tin ảnh hưởng mức cao và nghiêm trọng kể trên.

Trong trường hợp xác định bị ảnh hưởng, các đơn vị cần khẩn trương cập nhật bản vá để kịp thời tránh nguy cơ bị tấn công mạng từ khai thác các lỗ hổng an toàn thông tin.

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

Đức Anh