

Cảnh báo 6 lỗ hổng bảo mật trong sản phẩm của Microsoft

19:04 23/03/2023

Cục An toàn thông tin, Bộ Thông tin và Truyền thông vừa đưa ra cảnh báo về 6 lỗ hổng bảo mật trong sản phẩm của Microsoft dựa trên danh sách bản vá tháng 03/2023.



Ảnh minh họa. (Ảnh: internet)

Theo đó, Cục An toàn thông tin cũng đề nghị các cơ quan, tổ chức rà soát để phát hiện hệ thống bị ảnh hưởng tránh nguy cơ bị tấn công.

6 lỗ hổng được đề cập tới gồm: CVE-2023-23392 tồn tại trong HTTP Protocol Stack, CVE-2023-23415 trong Internet Control Message Protocol, CVE-2023-23399 trong Microsoft Excel và CVE-2023-23400 trong Windows DNS Server, lỗ hổng CVE-2023-23397 trong Microsoft Outlook và lỗ hổng CVE-2023-24880 trong Windows SmartScreen.

Đặc biệt, cần chú ý lỗ hổng CVE-2023-23397 cho phép thực hiện tấn công nâng cao đặc quyền, lỗ hổng CVE-2023-24880 cho phép đối tượng thực hiện tấn công vượt qua cơ chế bảo mật là 2 lỗ hổng đang bị đối tượng tấn công khai thác

trong thực tế. 4 lỗ hổng còn lại đều cho phép đối tượng tấn công thực thi mã từ xa.

Do đó, các đơn vị cần tiến hành kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng, nếu phát hiện lỗi cần kịp thời cập nhật bản vá để tránh nguy cơ bị tấn công mạng.

Bên cạnh đó, cũng cần tăng cường 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 cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời nguy cơ tấn công mạng.

Khi cần hỗ trợ, các đơn vị có thể liên hệ tới Cục An toàn thông tin Trung tâm Giám sát an toàn không gian mạng quốc gia (số điện thoại 02432091616, thư điện tử: ais@mic.gov.vn) để được trợ giúp.

Hà Trần