TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Cảnh báo về các lỗ hổng bảo mật mức cao trong những sản phẩm Microsoft

10:06 11/03/2022

Cục An toàn thông tin, Bộ Thông tin và Truyền Thông vừa có cảnh báo về các lỗ hổng bảo mật mức cao trong những sản phẩm Microsoft công bố tháng 03/2022.



Ảnh minh hoạ. (Ảnh: internet)

Cảnh báo được Bộ Thông tin và Truyền thông (TT&TT) gửi tới đơn vị chuyên trách về CNTT của bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ; Sở TT&TT của tỉnh, thành phố trực thuộc Trung ương, tập đoàn, tổng công ty nhà nước, ngân hàng, tổ chức tài chính và hệ thống đơn vị chuyên trách về an toàn thông tin.

Cơ quan này cho hay, ngày 08/03, Microsoft đã phát hành danh sách bản vá tháng Ba với 71 lỗ hổng bảo mật trong các sản phẩm của mình. Trong 71 lỗ hổng mới được Microsoft công bố và phát hành bản vá, Cục An toàn thông tin đề nghị các cơ quan, đơn vị, doanh nghiệp đặc biệt chú ý 8 lỗ hổng bảo mật có mức ảnh hưởng cao.

Cụ thể, 2 lỗ hổng bảo mật CVE-2022-21990, CVE-2022-23285 tồn tại trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. Cùng có điểm CVSS là 8.8, hai lỗ hổng bảo mật này đến các máy dùng Windows Server 2008/2012/2016/2019/2022, Windows 10/8.1/7. Các lỗ hổng đã có mã khai thác được công bố rộng rãi trên Internet.

Cũng ảnh hưởng đến máy dùng Windows Server 2008/2012/2016/2019/2022 và Windows 11/10/8.1/7, lỗ hổng bảo mật CVE-2022-24459 trong Windows Fax và Scan Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

Lỗ hổng bảo mật CVE-2022-24508 trong SMBv3 cho phép đối tượng tấn công thực thi mã từ xa trên Windows SMBv3 Client/Server. Lỗ hổng này ảnh hưởng đến các máy dùng Windows 10/11, Windows Server 2022.

Lỗ hổng bảo mật CVE-2022-23277 trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ; ảnh hưởng các máy dùng Microsoft Exchange Server 2019/2016/2013.

Có điểm CVSS là 7, lỗ hổng bảo mật CVE-2022-21967 tồn tại trong Xbox Live Auth Manager for Windows cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

Trong khi đó, lỗ hổng bảo mật CVE-2022-22006 trong HEVC Video Extensions cho phép đối tượng tấn công thực thi mã từ xa; và lỗ hổng bảo mật CVE-2022-24501 trong VP9 Video Extensions cũng cho phép đối tượng tấn công thực thi mã từ xa.

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

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 (NCSC) theo số điện thoại 02432091616 và thư điện tử ais@mic.gov.vn

Hà Trần