

MICROSOFT VÁ LỖ HỔNG NGUY HIỂM MỚI TRONG VISTA

Micros

Microsoft vừa mới cho sửa một lỗ hổng nghiêm trọng khác trong Vista xuất hiện từ cuối lễ Giáng sinh. Sự chậm trễ này cũng tương tự như quy trình xử lý lỗ hổng tro chuột động, từng trở thành tâm điểm bảo mật tháng 4/2007 sau khi giúp tin tặc đột nhập vào hệ thống.

Lỗ hổng mới liên quan tới cách thức trình Client/Server Run-time Subsystem (CSRSS) của hệ điều hành xử lý các thông điệp lỗi. Ngoài Vista, lỗ hổng này còn ảnh hưởng tới cả Windows 2000 SP4 và Windows XP.

Theo như Microsoft thì lỗ hổng này không nghiêm trọng bằng lỗ hổng tro chuột bởi người dùng cần phải thực hiện một loạt các tác vụ trên website độc hại thì cuộc tấn công mới diễn ra được. Lỗ hổng có thể cho phép tin tặc thực thi mã nhị phân trên hệ thống ảnh hưởng.

Ngoài bản vá mới nhất cho Vista, Microsoft còn sửa chữa một lỗ hổng nghiêm trọng trong công nghệ Agent của Windows 2000 SP4 và Windows XP SP2. Tin tặc có thể khai thác sai sót bảo mật này thông qua IE6 nếu người dùng truy cập vào một trang web độc hại. Vista và IE7 không bị ảnh hưởng bởi lỗ hổng này.

Dưới đây là thông tin về một số lỗ hổng nghiêm trọng được vá gần đây:

Ảnh độc hại

Ứng dụng Photoshop CS2 và CS3 của Adobe cũng chứa những lỗ hổng nghiêm trọng, có thể cho phép kẻ tấn công kiểm soát toàn bộ máy tính nạn nhân nếu họ sử dụng những chương trình này để các ảnh bitmap (đuôi .bmp, .dib, hoặc .rle) đã bị tin tặc chỉnh sửa (cài đặt mã độc). Theo hãng bảo mật Secunia và Nhóm phản ứng bảo mật khẩn cấp của Pháp (FSIRT), ít nhất đã có một mã khai thác lỗ hổng này xuất hiện trên mạng Internet. Hiện tại Adobe vẫn chưa phát triển bản patch cho lỗ hổng này, vì vậy người dùng cần phải cẩn thận khi mở các e-mail hoặc download ảnh không rõ nguồn gốc.

Trong khi đó, một chuyên gia nghiên cứu bảo mật độc lập đã đoạt giải thưởng 10.000USD trong cuộc thi hack hệ điều hành Mac OS X. Chuyên gia này đã khai thác một lỗ hổng mới trong trình QuickTime của Apple để đột nhập vào Mac OS X. Apple đã phát triển và đưa ra bản patch cho lỗ hổng này (ảnh hưởng tới cả Windows) sau 11 ngày kể từ khi nó bị phát hiện. Bản nâng cấp

QuickTime 7.1.6 cũng đã được sửa để "miễn nhiễm" với lỗ hổng mới.

Vista xung đột với iPod

Microsoft cũng đã sửa một lỗi trong Vista để hệ điều hành này không tác động tiêu cực tới thiết bị nghe nhạc này khi người dùng sử dụng chức năng "Safely Remove Hardware" để ngắt kết nối iPod. Mặc dù Microsoft không cung cấp thông tin chi tiết về cách thức lỗ hổng ảnh hưởng tới iPod nhưng hãng này khuyến nghị người dùng nên sử dụng tính năng iTunes để khôi phục nhạc trên iPod nếu có xảy ra sự cố. Đồng thời, Microsoft khuyên người dùng luôn sử dụng iTunes để ngắt kết nối iPod với máy tính.

Yahoo Messenger phát sinh lỗi

Trình tin nhắn tức thời này tồn tại một trình điều khiển ActiveX "có vấn đề" khiến cho người dùng đứng trước nguy cơ tấn công khi họ xem một trang web độc hại. IE7 và Vista vẫn bị tác động bởi lỗ hổng này tuy mức độ có phần nhẹ đi. Theo Yahoo, bất cứ phiên bản YM 8.x nào trước thời điểm 13/3/2007 đều bị ảnh hưởng. Người dùng nên cập nhật bản nâng cấp YM mới nhất.

Series lỗi của Apple

Apple đã vá tổng cộng 25 lỗ hổng trong hệ điều hành OS X sau một tháng kể từ khi hãng này sửa chữa tới 45 lỗ hổng nguy hiểm khác.