LỖI QUICKTIME ĐE DOẠ XP, VISTA

Mã tấn

Mã tấn công một lỗi bảo mật chết người chưa được khắc phục trong ứng dụng QuickTime của Apple mới đây đã lại được tung lên mạng.

Ông Krystian Kloskowski – một chuyên gia bảo mật rất có uy tín của Symantec – là người phát hiện ra lỗi QuicTime này và đã chính thức cho công bố rộng rãi hồi cuối tuần trước. Đúng một ngày sau khi công bố lỗi, Kloskowski cùng với một chuyên gia nghiên cứu khác đã cho công bố mã khai thác lỗi.

Mã khai thác nói trên được chứng thực có đủ khả năng tấn công QuickTime phiên bản 7.2 và 7.3 chạy trên nền tảng Windows XP SP2 hoặc Windows Vista. Lỗi bắt nguồn từ phương thức xử lý Real Time Streaming Protocol (RTSP) - thủ tục liên kết trình diễn tệp tin audio/video luồng trực tuyến (streaming).

Ngày 26/11, hãng bảo mật Symantec xác nhận phiên bản QuickTime cho Mac OS X cũng mắc lỗi tương tự như trên. Mã khai thác được chuyên gia Kloskowski công bố nói trên cũng hoàn toàn có thể được sử dụng để tấn công QuickTime trên Mac OS.

Symantec cho biết tin tặc có thể tấn công người dùng bằng cách lừa họ truy cập vào một website độc hại có lưu trữ tệp tin audio/video streaming "cấy" mã khai thác hoặc lừa họ nhắp chuột để mở một tệp tin QTL đính kèm theo email.

Nếu khai thác thành công lỗi bảo mật này tin tặc sẽ có thể "nhồi nhét" thêm nhiều mã độc lên hệ thống mắc lỗi và ăn cắp được rất nhiều thông tin cá nhân của người dùng. Còn nếu không thành công thì tin tặc cũng sẽ làm treo cứng luôn QuickTime.

Chuyên gia bảo mật cộng tác cùng Kloskowski cho biết phiên bản QuickTime chạy trên Vista dễ bị tấn công hơn trên Windows XP. Nguyên nhân là bởi QuickTimePlayer không tích hợp cơ chế Address Space Layout Randomization (ASLR) cấp bộ nhớ vận hành như của Vista.

Ba tuần trước đây Apple cũng đã phát hành bản cập nhật để sửa một loạt lỗi trong phiên bản QuickTime 7.3 liên quan đến tính năng xử lý hình ảnh và Java. Tính chung từ đầu năm đến nay Apple đã phải khắc phục tổng cộng 31 lỗi bảo mật QuickTime.

Hoàng Dũng