

CÁC LỖ HỔNG CỦA HỆ ĐIỀU HÀNH MAC NGUY HIỂM ĐỐI VỚI NGƯỜI SỬ DỤNG

Tom Ferris, chuyên gia nghiên cứu về bảo mật ở Mission Viejo (bang California), là người đầu tiên đưa ra thông tin về 7 lỗ hổng bảo mật trong hệ điều hành của Apple. Ferris cho biết, các hacker có thể khai thác những lỗ hổng nguy hiểm để chạy các đoạn mã độc hại trên máy tính của nạn nhân.

Tom Ferris, chuyên gia nghiên cứu về bảo mật ở Mission Viejo (bang California), là người đầu tiên đưa ra thông tin về 7 lỗ hổng bảo mật trong hệ điều hành của Apple. Ferris cho biết, các hacker có thể khai thác những lỗ hổng nguy hiểm để chạy các đoạn mã độc hại trên máy tính của nạn nhân. Phản ứng lại những thông tin do Ferris công bố, Bud Tribble, Phó chủ tịch phụ trách phần mềm của Apple phát biểu: “Chúng tôi đang nghiên cứu để khắc phục những lỗ hổng này”. Ông cũng không quên trấn an người sử dụng: “Tôi nghĩ rằng điều quan trọng là mặc dầu có các nguy cơ tiềm tàng nhưng hiện nay chưa có lỗ hổng nào bị khai thác và cũng chưa có khách hàng nào bị ảnh hưởng từ những lỗ hổng này”. Năm trong số những lỗ hổng Ferris chỉ ra liên quan tới cách xử lý các tệp hình ảnh (bao gồm các định dạng BMP, TIFF và GIF) của hệ điều hành. Trong số hai lỗ hổng còn lại, một lỗ hổng liên quan tới quá trình hệ điều hành giải các tệp nén dưới dạng .zip. Lỗ hổng cuối cùng liên quan tới trình duyệt Safari của Apple.

“Lỗi liên quan tới xử lý ảnh là nghiêm trọng nhất. Các hacker có thể khai thác lỗi này để kiểm soát máy tính và thi hành các đoạn mã độc hại mà người dùng khó có thể phát hiện”, Ferris nói. Ferris còn cho biết thêm, Apple đã âm thầm vá một trong những lỗi liên quan tới xử lý tệp ảnh TIFF trong bản cập nhật số 10.4.6. Đây cũng là lỗi duy nhất hiện nay Apple đã xử lý. Ferris cũng chính là người đã phát hiện và công bố thông tin về một số lỗ hổng trong một số sản phẩm khác của Apple như iTunes và QuickTime. Ngoài ra, ông cũng là chuyên gia bảo mật đã phát hiện một số lỗi khá nghiêm trọng trong Firefox - trình duyệt được sử dụng nhiều thứ hai, sau trình duyệt IE của Microsoft.