HÀNG LOẠT TRÌNH DUYỆT WEB MẮC LỖI BẢO MẬT

Hôm 06/06, rất nhiều các hãng bảo mật ra cảnh báo về một lỗ hổng bảo mật tồn tại trong một loạt trình duyệt web khác nhau có thể bị lợi dụng để ăn cắp thông tin. Theo cảnh báo này, hàng loạt các loại trình duyệt web như Internet Explorer, Firefox, Mozilla v&agr

Hôm 06/06, rất nhiều các hãng bảo mật ra cảnh báo về một lỗ hổng bảo mật tồn tại trong một loạt trình duyệt web khác nhau có thể bị lợi dụng để ăn cắp thông tin. Theo cảnh báo này, hàng loạt các loại trình duyệt web như Internet Explorer, Firefox, Mozilla và SeaMonkey vận hành trên nền tảng Windows, Linux và Mac đều bị ảnh hưởng bởi lỗ hổng lọc khoá JavaScript. Một kẻ tấn công chủ tâm có thể lợi dụng lỗ hổng này để ăn cắp các thông tin các nhân của người sử dụng như thông tin tài khoản tín dụng, ngân hàng trực tuyến ... Riêng hãng bảo mật Symantec, cuối ngày hôm qua, đã cảnh báo mọi phiên bản trình duyệt Internet Explorer và Firefox đều bị ảnh hưởng bởi lỗ hổng bảo mật này. "Vấn đề ở đây là một kẻ tấn công chủ tâm có thể lợi dụng sự kiện onKeyDown của ngôn ngữ lập trình máy khách JavaScript để ghi nhận mọi hoạt động bàn phím của người sử dụng," Symantec cảnh báo. Chính vì thế mà kẻ tấn công có thể lợi dụng lỗ hổng bảo mật này để lọc ra những hoạt động bàn phím khi người sử dụng xử lý một form mẫu trên web đưa vào một hộp thoại tải tệp tin lên "vô hình" nằm trên chính trang web đó. Các thông tin ngay sau đó sẽ được gửi về cho kẻ tấn công. "Để khai thác thành công lỗ hổng bảo mật này thì kẻ tấn công phải buộc người dùng phải nhập bằng tay toàn bộ đường dẫn đầy đủ của tệp tin mà chúng muốn tải xuống hoặc một số hoạt động bàn phím cụ thể từ phía nạn nhân. Chính vì thế mà lỗ hổng bảo mật có thể sẽ trở thành một công cụ tấn công hiệu quả những người chơi game trên web, blog hoặc những trang web tương tự cần phải có người dùng nhập thông tin từ bàn phím," Symantec cho biết. Trong khi đó, hãng bảo mật Secunia chỉ xếp lỗ hổng bảo mật này vào mức độ "kém nghiêm trọng" - nấc thang thứ 2 từ dưới lên trong chiếc thang 5 bậc đo mức độ nguy hiểm của các lỗi bảo mật. Đây là một lỗ hổng bảo mật không bình thường vì nó không chỉ ảnh hưởng đến riêng trình duyệt Internet Explorer - IE 6.0 được cài đặt đầy đủ các bản vá, thậm chí là cả IE 7.0 - mà còn cả Firefox hay một số trình duyệt của hãng khác như SeaMonKey. Nó cũng là lỗ hổng bảo mật đầu tiên ảnh hưởng đến các phiên bản trình duyệt trên một loạt các nền tảng khác nhau Windows, Linux, và Mac. Charles McAuley - người đầu tiên đã phát hiện ra lỗ hổng bảo mật này và công bố thông qua danh sách email bảo mật Full Disclosure hôm 05/06 - đã công bố một đoạn mã được chứng minh là có đầy đủ khả năng khai thác lỗi bảo mật này. Symantec khuyến cáo người sử dụng nên vô hiệu hoá tính năng JavaScript của trình duyệt. Hoàng Dũng