IE7 VÀ FIREFOX 2.0 CÓ CHUNG "TỬ HUYỆT"

Hai tr

Hai trình duyệt mới nhất là Internet Explorer 7 và Firefox 2.0 có chung một lỗi logic. Có vẻ như vụ việc này còn thực sự nghiêm trọng hơn khi hai phiên bản trình duyệt mới của Microsoft và Mozilla không phải là những "nạn nhân" duy nhất. Lỗi này có ảnh hưởng tới cả IE 5.01, IE6, IE7 và cả Firefox 1.5.0.9. Microsoft đã từng nhấn mạnh rằng IE7 trên Windows Vista sẽ không bị tấn công theo bất kỳ cách thức nào.

Michal Zalewski, người phát hiện ra "tử huyệt" của IE7, cho biết: "Trong số tất cả các trình duyệt hiện đại, các miền dạng (được sử dụng để upload những dữ liệu người sử dụng tới một server ở xa) có tính năng bảo vệ bổ sung nhằm ngăn các đoạn script chọn lựa ngẫu nhiên các file nội bộ gửi đi, và tự động chấp nhận định dạng mà người sử dụng không hề biết. Ví dụ, thông số dạng ".value" không thể được lập hay thay đổi. và bất kỳ thay đổi nào sang dạng ".type" sẽ reset lại nội dung của miền."

Trong trường hợp các lỗi này bị khai thác thành công, thì tác động của người sử dụng là cần thiết. Trong trường hợp này, người sử dụng sẽ phải truy cập vào các vùng bị "nhiễm" của một trang Web, cả bằng IE hay Firefox. Zalewski giải thích rằng các phím nhập ở các vị trí không có liên quan có thể bị kẻ tấn công đưa vào "tầm ngắm".

Để kiểm chứng hoạt động của "tử huyệt" trong IE7, hãy click vào http://lcamtuf.coredump.cx/focusbug/ieversion.html. Nội dung tương tự đối với Firefox có thể tìm thấy tại http://lcamtuf.coredump.cx/focusbug/ffversion.html. "Cả hai ví dụ này đều dành riêng cho Windows và yêu cầu C:BOOT.INI để tồn tại và để người sử dụng đọc được. Nguy cơ tấn công không bị giới hạn ở bất kỳ hệ điều hành nào, nhưng tôi quyết định cung cấp một nguy cơ dành cho hệ điều hành desktop phổ biến nhất – các bản *nix truy cập /etc/hosts hoặc /etc/passwd rất dễ phát triển." Zalewski bổ sung.

Nguyễn Nam