LỖI BẢO MẬT LIÊN THÔNG IE & FIREFOX

Hãng b

Hãng bảo mật Secunia cho biết vừa lỗi bảo mật vừa được phát hiện trong Internet Explorer 7 không chỉ ảnh hưởng đến phiên bản trình duyệt này mà còn cả IE 6 và Firefox phiên bản 1.5 và 2.0.

Đây hoàn toàn không phải là một lỗi bảo mật mà là một lỗi đã từng là các chuyên gia bảo mật đau đầu trong nhiều năm qua bởi đây là một lỗi bảo mật rất dễ bị lợi dụng. Chỉ cần bổ sung thêm một số mã Javascript "độc" là một trang web đã hoàn toàn có thể thay đổi địa chỉ cũng như nội dung được hiển thị trong cửa sổ pop-up.

Nếu trình duyệt được trang bị khả năng chống pop-up thì về lý thuyết mã khai thác lỗi nói trên sẽ bị vô hiệu hoá. Nhưng nếu trang web chứa mã khai thác lỗi được mở cùng lúc với một trang web an toàn cho phép bung pop-up thì mã khai thác lỗi sẽ vẫn hoạt động bình thường. Nếu tính năng chặn pop-up bị vô hiệu hoá thì nguy cơ bị tấn công sẽ càng cao hơn.

Liên thông

Trang tin điện tử chuyên về lĩnh vực CNTT BetaNews đã tiến hành thử nghiệm và đưa ra kết luận lỗi bảo mật nói trên không chỉ ảnh hưởng đến phiên bản IE 7 mà còn cả phiên bản IE 6, Firefox 1.5 và 2.0. Không những thế BetaNews còn khai thác thành công lỗi bảo mật đó trên Firefox 1.5 với tính năng chặn pop-up đã được kích hoạt.

Secunia cho biết chịu ảnh hưởng nặng nề nhất có lẽ là IE 7. "Chúng tôi đã tiến hành kiểm tra và đi đến kết luận đây là một lỗi bảo mật chèn cửa số (Windows Injection Vulnerability)."

Khi lỗi bảo mật Windows Injection Vulnerability lần đầu tiên được phát hiện, giải pháp mà Microsoft đưa ra là bổ sung thêm môt loạt các lựa chọn thiết lập bảo mật vào Internet Options cho IE 6. Bằng cách truy cập vào thẻ Internet Options | Security và nhắp chuột vào Custom Level, tìm đến dòng 'Navigate sub-frames across different domains' và nhắp chuột lựa chọn 'Disable' lỗi bảo mật sẽ được vô hiệu hoá. Mặc định IE 7 đã được cài đặt thiết lập này.

Thử nghiệm trên một PC chạy Windows XP, trình duyệt IE 7 với cấu hình mặc định như trên đã trót lọt vượt qua cuộc thử thách trước lỗi bảo mật nói trên ngay cả khi tính năng chặn pop-up bị vô hiệu hoá. Nhưng với các hệ thống Windows XP khác thì kết quả lại không hề xuôn xẻ như vậy. IE

7 vẫn hoàn toàn có thể bị tấn công.

Trong khi đó, Firefox 1.5 và 2.0 đã thất bại hoàn toàn trước các cuộc thử nghiệm. Chỉ riêng Firefox 2.0 chạy trên Windows Vista RC 2 là vượt qua cuộc thử nghiệm.

Tuy nhiên, hiện vẫn còn khá nhiều thắc mắc xung quanh vấn đề mà Secunia nêu ra. Bởi về lý thuyết thì các cấu hình bảo mật cho các trang web được duyệt trong trình duyệt cũng được áp dụng đối với các cửa sổ pop-up. Điều này đồng nghĩa với việc nếu cửa sổ pop-up có chứa mã độc hại thì theo lý thuyết nó cũng bị chặn.

Hoàng Dũng