PHÁT HIỆN HAI LỖ HỔNG MỚI TRONG FIREFOX

Hãng b

Hãng bảo mật SecuriTeam vừa công bố hai lỗ hổng mới trong trình duyệt Mozilla Firefox, có thể cho phép lưu các file của tin tặc về máy tính để kích hoạt cuộc tấn công.

Lỗ hổng thứ nhất nằm trong tính năng khoá pop-up của Firefox. Thông thường, Firefox không cho phép website truy cập vào các file được lưu trữ cục bộ; tuy nhiên tính năng kiểm định này lại không thể hoạt động nếu người dùng Firefox tự ý tắt tính năng khoá pop-up của trình duyệt. Kết quả là kẻ tấn công có thể sử dụng lỗ hổng này để đánh cắp các tệp tin lưu trữ trên ổ cứng và các thông tin cá nhân lưu giữ trong đó.

Ngữ cảnh của lỗ hổng trên được mô tả như sau: kẻ tấn công sẽ dụ dỗ người dùng nhấn vào một đường link độc hại có file gốc kết nối với mã khai thác trên ổ cứng máy tính nạn nhân. Sau đó, sẽ có một cửa sổ thông báo hỏi người dùng có cho phép cửa sổ pop-up xuất hiện để xem file video hoặc download file hay không. Khi đó tệp tin do tin tặc cung cấp sẽ được tải về máy tính nhờ lỗ hổng của trình duyệt, và cho phép tin tặc có thể đoạt quyền đọc các file cục bộ trên máy tính nạn nhân.

SecuriTeam cho biết lỗ hổng thứ nhất chỉ ảnh hưởng tới các phiên bản Firefox cũ (trừ phiên bản Firefox 2.0 mới nhất).

Còn đối với lỗ hổng thứ hai, SecuriTeam cho rằng nó liên quan tới tính năng chống phishing của Firefox. Với lỗ hổng này, một phisher có thể lừa trình duyệt tin rằng một site giả mạo đã được bảo mật bằng cách chèn các ký tự đặc biệt vào đường URL của website. Lỗ hổng được xác định ảnh hưởng tới các phiên bản Firefox cũ.

Hiện tại Mozilla vẫn chưa có bất cứ bình luận vào về các thông tin trên.