GOOGLE DESKTOP SƠ HỞ VÀ BỊ TẤN CÔNG

Lỗ hổn

Lỗ hổng cho kiểu tấn công dựa trên web còn ít người biết (gọi là "anti-DNS pinning") có thể cho phép tin tặc truy cập được vào bất kì dữ liệu nào mà Google Desktop đánh chỉ mục. Đây là lần thứ hai trong vòng một tuần, lỗ hổng bảo mật trong Google Desktop bị người ta nhắc tới.

Phần mềm tìm kiếm PC của Google bị "hở sườn" trước kiểu tấn công "anti-DNS pinning". Theo các nhà nghiên cứu bảo mật, kiểu tấn công này có thể cho phép tin tặc truy cập được vào bất kì dữ liệu nào được Google Desktop đánh chỉ mục.

Đây là lần thứ hai trong vòng một tuần, lỗ hổng bảo mật trong Google Desktop bị người ta nhắc tới. Hôm 21/2/2007, các nhà nghiên cứu của Watchfire cho biế đã phát hiện ra lỗ hổng bảo mật có thể cho phép tin tặc đọc các file hoặc chạy phần mềm trái phép trên các hệ thống đang chạy Google Desktop.

Theo nhà nghiên cứu bảo mật độc lập Robert Hansen (người đầu tiên phát hiện ra kiểu tấn công này), để tấn công được, đầu tiên tin tặc cần khai thác lỗ hổng kịch bản chéo trang (cross-site scripting) trong website Google.com nhưng hậu quả thì nghiêm trọng hơn nhiều. Ông nói, "giờ đây, tất cả dữ liệu trên máy tính chạy Google Desktop có thể bị "hút sạch" về máy tính của tin tặc

Ông Hansen cho biết, Google không phải là công ty duy nhất bị thương tổn bởi các vụ tấn công dựa trên web. Đầu tháng 12/2006, MySpace.com đã bị một worm lan truyền trong cộng đồng MySpace nhằm đánh cắp thông tin đăng nhập và xúc tiến các website quảng cáo.