

NGƯỜI DÙNG YAHOO 360 DỄ BỊ LỪA TỰ TAY XÓA BLOG

Một lỗi

Một lỗi trong hệ thống nhật ký online được chú ý nhất hiện nay ở VN có thể bị kẻ xấu lợi dụng để chơi khăm người khác bằng cách dụ họ bấm vào đường link dạng câu lệnh xóa nội dung trong blog của nạn nhân. Người mắc bẫy sẽ tự "ra tay" với những dòng tâm huyết của mình hoặc chia sẻ từ bạn bè.

Phát hiện ra lỗi hổng này, Nguyễn Ngọc Long, Quản trị mạng tại một doanh nghiệp CNTT lớn trong nước, mô tả đây là lỗi CSRF (Cross Site Request Forgery), phương pháp mượn tay người khác để thực hiện một hành động không được phép.

Thay vì thiết lập một cơ chế minh bạch cho các thao tác xóa, sửa nội dung thông tin để tránh xảy ra việc xóa nhầm, nhà cung cấp dịch vụ Yahoo 360 đã không thiết kế riêng một trang quản trị mà tất cả thông qua cookie và session... nhằm làm giản tiện cho người dùng. Vì vậy, nếu ai đó muốn chơi xấu là xóa một entry hay comment trên blog của người khác, sẽ chuẩn bị một link có tham số là xóa một nội dung theo định dạng của blog đó rồi tìm cách dụ nạn nhân bấm vào. Khi đó, nếu nạn nhân đang trong tình trạng login sẵn vào blog của mình (có nghĩa là cookie và session... đã lưu sẵn ở trên máy), mà mắc bẫy sẽ chủ động xóa nội dung được chỉ định trong link.

Kẻ xấu có thể khiến nạn nhân tự tay xóa thông tin trên blog của mình. Ảnh VNE.

Trung tâm An ninh mạng BKIS nhận định kẻ xấu có thể khai thác lỗi này để tấn công vào blog của người sử dụng. Tuy nhiên, "việc ném đá giấu tay" dạng này chỉ có thể dừng lại ở việc tấn công

từng blog chứ chưa thể "tàn phá" trên diện rộng vì muốn "nhắm" blog nào phải chuẩn bị riêng link nguy hại cho site đó.

Nguyễn Ngọc Long cho biết đã gửi cảnh báo về lỗ hổng này đến nhóm quản trị của Yahoo 360 nhưng chưa thấy có hồi âm nào. "Theo tôi, người dùng Yahoo 360 tạm thời không nên đăng nhập vào 'ngôi nhà ảo' của mình hay của người khác trước khi lỗi này được nhà cung cấp chỉnh sửa", Long nói.

Ông Vũ Ngọc Sơn, chuyên gia của BKIS, cũng khuyến cáo: "Trong thời gian chờ đợi Yahoo 360 thắt chặt hơn mức an toàn cho các blog cá nhân, người sử dụng nên cẩn thận hơn với các link lạ, đồng thời nên backup những bài viết quan trọng của mình".

Nguyễn Hằng