# RSS CÓ THỂ BỊ LỢI DỤNG LÀM CÔNG CỤ TẤN CÔNG

Các chuyên gia bảo mật cảnh báo các luồng tin RSS (RSS Feed) có thể bị lợi dụng để tấn công các hệ thống PC không được bảo vệ. Thông tin nói trên đã được chuyên gia bảo mật Robert Auger của SPI Dynamics đưa ra công bố tại Hội nghị Black Hat năm nay. Chuy&ecir

Các chuyên gia bảo mật cảnh báo các luồng tin RSS (RSS Feed) có thể bị lợi dụng để tấn công các hệ thống PC không được bảo vệ. Thông tin nói trên đã được chuyên gia bảo mật Robert Auger của SPI Dynamics đưa ra công bố tại Hội nghị Black Hat năm nay. Chuyên gia Auger nhấn mạnh đây là một vấn đề có ảnh hưởng thực sự nguy hiểm đến các luồng thông tin RSS. Tin tặc chỉ cần bổ sung thêm một số đoạn mã JavaScript độc hại và các RSS Feeds là đã có thể tấn công người dùng. SPI Dynamics khẳng định mọi ứng dụng đọc RSS Feed - cho dù đó là phần mềm ứng dụng trên máy tính hay là ứng dụng trực tuyến trên web - đều có thể bị tấn công bằng phương thức nói trên. Thông qua những cuộc tấn công như thế này kẻ tấn công có thể ăn cắp được các thông tin nhạy cảm như mật khẩu hay dữ liệu cá nhân của người dùng. Nguy hiểm hơn là những vụ tấn công như vậy có thể bắt nguồn từ các trang web đáng tin cậy. Một số trang web Blog hiện cho phép người dùng gửi ý kiến trực tiếp đính kèm theo các các RSS Feed. Đây chính là cách có thể bị tin tặc lợi dụng để bổ sung các đoạn mã JavaScript vào trong các luồng thông tin RSS. Hoặc tin tặc có thể mở một trang web Blog riêng của mình và phát tán các luồng RSS nguy hiểm. Đây là cách mà chuyên gia Auger tin rằng sẽ là cách tấn công phổ biến nhất của tin tặc. Đối với ứng dụng RSS trên web, Bloglines được xem là ứng dễ bị tấn công nhất. Trong khi đó, RSS Reader, RSS Owl, Feed Demon, và Sharp Reader chính là những phần mềm RSS dễ phải đối mặt với các vụ tấn công nhất. Để bảo vệ hệ thống, chuyên gia Auger khuyến cáo người dùng nên vô hiệu hoá tính năng cho phép chạy các scripts, applets, và plug-ins trong ứng dụng RSS. Hoàng Dũng