MARE.D TẤN CÔNG HỆ THỐNG QUẢN LÍ NỘI DUNG MAMBO

F-Secure đang cảnh báo về "sâu mạng" (network worm) Mare.D nhắm vào các điểm dễ thương tổn trong hệ thống quản lí nội dung (Content Management System - CMS) Mambo và thư viện PHP XML-RPC (đây là thư viện mã cho người lập trình PHP cho phép các thủ tục chạy

F-Secure đang cảnh báo về "sâu mạng" (network worm) Mare.D nhắm vào các điểm dễ thương tổn trong hệ thống quản lí nội dung (Content Management System - CMS) Mambo và thư viện PHP XML-RPC (đây là thư viện mã cho người lập trình PHP cho phép các thủ tục chạy giữa nhiều máy tính với các hệ điều hành khác nhau.

Giao diện của hệ thống CMS Mambo

F-Secure cho biết, sâu Mare.D cài đặt một số cổng hậu (backdoor) lên hệ thống bị nhiễm (và sẽ gây hại nếu hệ thống có chạy hệ thống CMS mã nguồn mở Mambo hoặc thư viện PHP XML-RPC). Hai trong số những cổng hậu này thuộc loại "connectback shell backdoor", có tên là "cb" và "ping.txt". Hai cổng hậu này kết nối với máy tính ở xa qua cổng 8080. Cổng hậu thứ ba được viết bằng ngôn ngữ Perl và được IRC (Internet Relay Chat) điều khiển. Thành phần chính của sâu nghe các lệnh ở cổng 27015 của giao thức UDP (User Datagram Protocol). Secunia nói, điểm dễ thương tổn này ảnh hưởng tới thư viện PHP XML-RPC phiên bản 1.1 và các phiên bản trước đó. Công ty khuyên người dùng nên nâng cấp thư viện PHP XML-RPC lên phiên bản 1.1.1. Trên website của mình, Mambo cho biết đã đưa ra các bản sửa lỗi cho 2 phiên bản 4.5.3 và 4.5.3h. Người dùng có thể tải các bản sửa lỗi này về từ địa chỉ http://www.mamboserver.com/. Mambo cũng khuyên người dùng nên nâng cấp phần mềm của mình nếu họ đang có phiên bản trước 4.5.3. Một nhà tư vấn của công ty Sophos nói, họ vẫn chưa thấy khách hàng nào phàn nàn về sâu Mare.D cả.