APACHE PHÁT SINH LỖ HỔNG NGUY HIỂM

Hãng Secunia vừa dẫn lời một chuyên gia nghiên cứu bảo mật độc lập cho biết đã phát hiện một lỗ hổng khá nguy hiểm trong phần mềm Apache. Đó là dạng lỗ hổng trong ứng dụng Apache HTTP Server, có thể cho phép tin tặc khởi phát các cuộc tấn công ở dạng kịch bản li

Hãng Secunia vừa dẫn lời một chuyên gia nghiên cứu bảo mật độc lập cho biết đã phát hiện một lỗ hổng khá nguy hiểm trong phần mềm Apache. Đó là dạng lỗ hổng trong ứng dụng Apache HTTP Server, có thể cho phép tin tặc khởi phát các cuộc tấn công ở dạng kịch bản liên miền (cross-site). Cũng theo Secunia, phần đầu (header) của thành phần đầu vào (input) "Expect:" trong Apache không được xử lý chặt chẽ trước khi trả về người dùng. Chính điểm yếu này đã cho phép tin tặc thực thi các dạng HTML nhị phân và mã kịch bản trên phiên trình duyệt của người dùng tại các site "có vấn đề" (thường là site giả mạo do tin tặc tạo ra). Lỗ hổng được xác định ảnh hưởng tới các phiên bản Apache 1.3.35, 2.0.58, và 2.2.2. Secunia cũng xây dựng mẫu thử nghiệm lỗ hổng này tại địa chỉ: http://secunia.com/expect_header_cross-site_scripting_vulnerability_test/