WINDOWS DÍNH LỖ HỔNG ZERO-DAY NGUY HIỂM CHƯA TỪNG THẤY

Lỗ hổn

Lỗ hổng mới thuộc hạng "cực kỳ nghiêm trọng", hiện diện bên trong tất cả các phiên bản Windows, ngoại trừ Windows 2003 và có dấu hiệu đang bị hacker khai thác.

Theo cảnh báo mới nhất của Microsoft, lỗ hổng này liên quan đến tính năng XMLHTTP 4.0 ActiveX Control bên trong Core Service 4.0. Công nghệ Core Service đảm bảo sự liên thông giữa các ứng dụng dựa trên nền chuẩn XML 1.0 với môi trường lập trình Jsript, VBScript và Visual Studio 6.0 của Microsoft.

Nguồn: breathedeeply

Microsoft cho biết họ đã ghi nhận được một số trường hợp tấn công "khoan sâu" vào lỗ hổng này. Hãng không tiết lộ mức độ nguy hiểm của lỗ hổng đến đâu, nhưng hãng bảo mật Secunia đã đánh giá lỗ hổng là loại "cực kỳ nghiêm trọng" (extremely Critical) - thang điểm cao nhất từ trước tới nay của hãng.

Theo Secunia, lỗ hổng cho phép kẻ tấn công giành toàn quyền kiểm soát hệ thống. Chúng có thể lừa người dùng truy cập vào một website được ngụy tạo rất khéo, hoặc thậm chí một trang phụ bên trong những diễn đàn ảo thông dụng kiểu như MySpace. Ngoài ra, chúng cũng có thể đăng quảng cáo trên một website trung gian và dụ người dùng click vào.

Mặc dù vậy, chủ tịch hãng bảo mật Sunbelt Software lại không có cùng quan điểm với Secunia. Ông này cho biết mới chỉ phát hiện được duy nhất vụ site khai thác lỗ hổng và lại là khai thác... không hiệu quả.

Microsoft đang tiến hành kiểm tra lỗ hổng trước khi quyết định có phát hành miếng vá khẩn cấp cho nó hay không. Nếu chỉ bị đánh giá là "nghiêm trọng trung bình", lỗ hổng này sẽ được bịt cùng với bản tin bảo mật phát hành tháng tới của Microsoft.

Trọng Cầm