LINUX NHIỀU LỖI GẤP 3 WINDOWS? NHẬN ĐỊNH VÔ CĂN CỨ!

Một công trình nghiên cứu mới đây của chính phủ Mỹ nhận định rằng số lỗ hổng bảo mật trong hệ điều hành nguồn mở Linux/Unix nhiều gấp ba lần hệ điều hành Windows không những bị cộng đồng nguồn mở chỉ trích, mà còn buộc không ít chuyên gia bảo mật phải ho&agr

Một công trình nghiên cứu mới đây của chính phủ Mỹ nhận định rằng số lỗ hổng bảo mật trong hệ điều hành nguồn mở Linux/Unix nhiều gấp ba lần hệ điều hành Windows không những bị cộng đồng nguồn mở chỉ trích, mà còn buộc không ít chuyên gia bảo mật phải hoài nghi. Bản tin An ninh mạng 2005 do Nhóm Phản ứng sự cố máy tính khẩn cấp của chính phủ Mỹ (CERT) công bố tuần trước, thống kê rằng trong số 5.198 lỗ hổng được ghi lại, 812 là của Windows, 2328 lỗ hổng thuộc về Linux/Unix và 2.058 lỗi rải rác ở các hệ thống khác. Có thực nguy hiểm gấp 3? Phản ứng trước báo cáo này, website NewsForge.com khẳng định số liệu của chính phủ đã có sự "lầm lẫn", vì nhiều bản báo cáo độc lập khác trước đây - tất nhiên là của các tổ chức ngoài nguồn mở tiến hành- đều kết luận Windows đầy rẫy lỗ hổng bảo mật nguy hiểm, dễ dàng bị các hacker khai thác. Trong khi lỗ hổng của Windows chỉ được thống kê ở các phiên bản XP, NT và 98, thì con số 2328 lại được tính gộp tất cả từ các hệ điều hành Solaris, AIX, HP-UX, BSD và Linux, cùng với 100 phiên bản khác nhau của hệ điều hành Chim cánh cụt này nữa. "Các tính tổng số lỗ hổng của CERT thật kỳ cục. Họ gộp chung toàn bộ lỗ hổng tìm thấy của Unix và Linux với nhau, trong khi con số này chả phản ánh được gì về tình hình bảo mật của riêng một hệ điều hành", Joe Brockmeier, tổng biên tập của Linux.com phản ứng gay gắt. Nguy cơ thật sự và Số liệu Lấy thí dụ, theo Joe, một lỗ hổng trong hệ điều hành Mac OS X không thể áp dụng vào Linux hay Unix, song bản báo cáo chính phủ đã không hề làm rõ điểm này. Chưa hết, trình duyệt Firefox cũng được xếp vào trong nền Linux, tính gộp tất cả lỗ hổng bảo mật của nó vào với Linux, dẫu trên thực tế, nó chạy trên nhiều hệ điều hành khác nhau. Chưa hết, theo Joe, nghiên cứu của CERT đã không hề chú ý đến mức độ nghiêm trọng của các lỗ hổng ghi nhận được, cũng như thời gian mà doanh nghiệp phát hành miếng vá là bao lâu. Graham Cluley, nhà tư vấn cao cấp của hãng bảo mật Sophos cũng nhận định rằng mức độ nghiêm trọng của một lỗ hổng, cũng như số lỗ hổng bị khai thác - là hai tiêu chí quan trọng nhất trong việc đánh giá sự an toàn của một hệ điều hành - chứ không phải kiểu tính gộp "thượng vàng hạ cám" nói trên. "Có nhiều lỗ hổng vụn vặt không có nghĩa là hệ điều hành này kém an toàn hơn hệ điều hành kia. Điều quan trọng là người ta phải xem với một lỗ hổng cụ thể, mức độ khai thác của hacker lớn hay nhỏ", ông nói. Đại bộ phận virus và Trojan máy tính vẫn chỉ nhắm đến hệ điều hành Windows mà thôi. Windows - Mục tiêu "ưa thích" nhất Nhà phân tích Andrew Jaquith của Yankee Group cho rằng cách "đếm số" lỗ hổng phần mềm theo kiểu của CERT là một cách tiếp cận vấn đề rất phiến diện và hời hợt, bởi vì nó chỉ căn cứ trên những lỗ hổng đã được công bố công khai trên mạng mà thôi. "Nó không thể đo được tình trạng bảo mật bản chất của hệ điều hành đó, nên tất yếu, không thể đưa ra được kết luận nào chính xác". Hệ điều hành Windows, với mức độ phổ biến hiện nay của nó, nói thế nào, vẫn cứ là mục tiêu tấn công ưa thích nhất của giới hacker và các phần mềm phá hoại malware. Khác với Microsoft, theo Joe, cộng đồng Linux có một cách tiếp cận khác với vấn đề bảo mật: sục sạo những lỗ hổng hiện có, đang còn tồn tại trong hệ thống. Còn Microsoft, trong khi đó, lại giữ kín mã nguồn sản phẩm của mình và chỉ phản ứng khi được thông báo về sự cố mà thôi. "Thông tin với dư luận là một việc tốt, nhưng nếu đưa thông tin một cách không thấu đáo như vậy chắc chắn sẽ khiến người dùng hoang mang và hiểu lầm bản chất vấn đề", Joe khẳng định. Thiên Ý