XU HƯỚNG LỖ HỔNG BẢO MẬT NỔI BẬT TRONG NĂM 2006

Theo s

Theo số liệu thống kê do SecurityFocus thu thập được từ bốn nguồn cơ sở dữ liệu bảo mật lớn, các lỗ hổng xuất hiện trong ứng dụng Web của năm 2006 tăng hơn 1/3 so với năm trước.

Hôm thứ hai, Computer Emergency Response Team (CERT) Coordination Center - Trung Tâm Phối Hợp Đội Phản ứng Nhanh Các Tình Huống Khẩn Cấp đã công bố số liệu thống kê cuối cùng về lượng lỗ hổng xác định được trong năm 2006. Dựa trên nguồn dữ liệu công cộng và dữ liệu riêng gửi trực tiếp tới CERT Coordination Center, nhóm này xác định được có tới 8.064 lỗ hổng bảo mật bị phát hiện trong năm vừa qua, tăng 35% so với năm 2005.

Ba cơ sở dữ liệu bảo mật lớn: National Vulnerability Database, Open-Source Vulerability Database và Symantec Vulnerability Database ghi nhận rằng phạm vi mở rộng của các lỗ hổng trong năm 2006 tăng từ 20 đến 35% so với năm 2005.

Yếu tố lớn nhất khiến lỗ hổng ngày càng trở nên phổ biến hiện nay là do việc phát hiện sai sót trong các ứng dụng Web thương mại và cộng đồng ngày càng trở nên dễ dàng, Art Manion - đội trưởng của CERT Coordination Center khẳng định.

"Điều tốt nhất chúng ta có thể nghĩ đến là hầu hết số lượng tăng đáng kể của lỗ hổng bảo mật là do khả năng 'dễ khám phá'. Chúng dễ tìm, dễ tạo và dễ triển khai".

"Nhiều người đang tiến hành nghiên cứu 'grep and gripe'. Họ thực hiện các cuộc tìm kiếm nhanh thông thường nhằm tìm ra một số kiểu mẫu hay mô hình. Nếu bắt gặp cái phù hợp, họ sẽ công bố rộng rãi. Nhưng đôi khi, kết cục cho quá trình này lại là các báo cáo sai".
(Steven Christey, biên tập viên của Common Vulnerabilities and Exposures Project, tức dự án CVE, chuyên khai thác và phát hiện các lỗ hổng phổ biến).

Sự gia tăng số lượng lỗ hổng trong năm 2006 không khiến nhiều nhà nghiên cứu bảo mật ngạc nhiên. Con số này tăng nhảy vọt so với năm 2005. Theo thống kê từ bốn nguồn cơ sở dữ liệu trên khẳng định, nguyên nhân chủ yếu là do các lỗi dễ tìm thấy trong ứng dụng Web. Theo Symantec, hãng sở hữu SecurityFocus thì trong nửa đầu năm 2006, hơn ¾ lỗ hổng phần mềm ảnh hưởng tới các ứng dụng trực tuyến. Một báo cáo hồi tháng 10 của Common Vulnerability and Exposures (CVE) Project tìm ra rằng ba loại lỗ hổng đứng đầu là ở các chương trình Web và trong 9 tháng đầu năm đã phát hiện ra 45% lượng lỗ hổng.

Quá trình tìm kiếm đơn giản thông qua mã nguồn hoặc dùng công cụ tìm kiếm mã của Google (Google code search) có thể lọc ra số lượng lớn các vấn đề bảo mật tiềm ẩn, thậm chí cho phép cả những kẻ mới học dò tìm sai sót cũng có thể chi ra được lỗ hổng bảo mật. Những người duy trì cơ sở dữ liệu bị ngập thông báo tìm được lỗ hổng của những người "sẽ là" các nhà nghiên cứu bảo mật. Họ dùng chương trình ghép xâu đơn giản để tìm ra vấn đề tiềm ẩn trong các ứng dụng nguồn mở, Steven Christey - biên tập viên của CVE Project do MITRE Cort, một tổ chức chính phủ phi lợi nhuận tài trợ nói.

"Nhiều người đang thực hiện nghiên cứu 'grep and gripe'". Đó là chương trình tìm kiếm linh hoạt grep, một phần phổ biến của các hệ thống "tựa Unix". "Họ tiến hành tìm kiếm nhanh thông thường nhằm tìm ra kiểu mẫu hay mô hình nào đó. Nếu bắt gặp cái phù hợp, họ sẽ công bố rộng rãi. Nhưng đôi khi, kết cục cho quá trình này lại là các báo cáo sai".

Khi những kẻ tập sự chú trọng vào ứng dụng Web thì các nhà nghiên cứu lâu đời hơn bắt đầu tập trung vào phần khác của hệ điều hành hay các chương trình ứng dụng phổ biến. Tool (chức năng hay công cụ), còn được biết đến với cái tên "fuzzer" là cách thức phổ biến ngày càng tăng được dùng để kiểm tra phần mềm xem có gặp vấn đề gì về dữ liệu đầu vào không. Các tool tìm kiếm lỗi rất hiệu quả và nhiều nhà nghiên cứu phải sử dụng thường xuyên đến chúng như một sách lược phát hiện lỗi sai mặc dù chúng gây nhiều tranh cãi.

"Bạn có một số mức phức tạp nổi bật cho các nhà nghiên cứu sai sót", Christey nói. "Bạn có nhiều người có thể tìm ra các lỗi nhỏ. Nhưng với phần mềm lớn và quan trọng, dường như khó khăn hơn rất nhiều cho các nhà nghiên cứu hàng đầu có thể tìm ra được vấn đề thực sự. Họ phải làm việc nhiều hơn, mất nhiều thời gian hơn, sử dụng nhiều tài nguyên hơn và thực hiện các nghiên cứu tổng hợp hơn".

Số lượng lỗi sai thống kê được trên các ứng dụng Web ngày càng tăng

Việc tìm kiếm lỗi hổng trong các ứng dụng trở nên dễ dàng khiến con số các lỗi sai tăng nhanh đáng kể trong năm 2006, hơn năm trước từ 20 đến 50%.

2006

2005

2004

2003

2002

2001

CERT/CC

8,064

5,990

3,780

3,784

4,129

2,437

NVD

6,604

4,877

2,367

1,281

1,959

1,672

OSVDB

8,500+*

7,187

4,629

2,632

2,184

1,656

Symantec

4,883

3,766

2,691

2,676

2,604

1,472

*OSDB ước tính từ quá trình thực hiện dữ liệu là đến nay số lượng lỗ hổng trong năm 2006 tăng hơn ít nhất là 20% so với năm 2005.
Nguồn: Computer Emergency Response Team Coordination Center (CERT/CC), National Vulnerability Database, Open-Source Vulerability Database và Symantec Vulerability Database.

Nhưng con số khổng lồ của năm 2006 không có nghĩa là Internet là nơi kém an toàn cho người dùng máy tính.

Nhiều ứng dụng Web có lỗi được tìm ra là các dự án cộng đồng, ít khi được dùng ra bởi các công ty lớn, Brian Martin - quản lý nội dung của Open-Source Vulnerability Database khẳng định.

"Các website cá nhân và những nơi lưu trữ kiểu 'mom-and-pop' dựa trên phần mềm chắc chắn sẽ bị ảnh hưởng, nhưng các công ty lớn hơn thì không".

Chương trình ứng dụng viết trên nền ngôn ngữ lập trình Web động phổ biến PHP được xác định chiếm tới 43% trong tổng số lỗ hổng của năm 2006. Ngôn ngữ này được dùng chủ yếu cho phần

mềm cộng đồng và các website nhỏ, nhưng một số gã khổng lồ danh tiếng như Yahoo!, Google cũng dùng PHP.
Trong khi lỗ hổng trong các ứng dụng Web chiếm số lượng lớn thì lỗ hổng trong hệ điều hành lại khiêm tốn đi nhiều, còn các ứng dụng client-side (dành cho máy khách) cũng tạo ra cú hích lớn hơn.

"Từ quan điểm của một hệ điều hành cốt lõi, chúng ta an toàn hơn. Nhưng thực tế là các mã độc hại vẫn chưa biến mất", Oliver Friedrichs - giám đốc trung tâm phản ứng bảo mật của Symantec nói. "Malware vẫn luôn nằm trên hệ thống của bạn. Nó chỉ không dùng các lỗ hổng phần mềm lõi để khai thác mà thôi".

Mặc dù chúng chỉ tạo ra một phần nhỏ trong toàn bộ số lượng lỗ hổng, nhưng các lỗ hổng chưa được biết đến trước đó (như zero-day chẳng hạn) trở thành đích nhắm của các cuộc tấn công hấp dẫn và là xu hướng lớn trong năm 2006.

"Đe doạ thực sự từ lỗ hổng zero-day là chúng được sử dụng thường xuyên vào mục đích nhắm tới các công ty và doanh nghiệp để lấy cắp thông tin, trong khi một lỗ hổng web đơn giản trên Internet không thể gây nhiều tác động quan trọng như vậy", Friedrichs chỉ rõ.