10 KHOẢNH KHẮC TỒI TỆ NHẤT CỦA NGÀNH BẢO MẬT

Tạp chí InformationWeek - một trong số những tạp chí về công nghệ thông tin hàng đầu thế giới – vừa cho công bố danh sách bình chọn 10 khoảnh khắc tồi tệ nhất của ngành bảo mật thế giới. 1. Lỗi bảo mật trong SQL Đúng một tuần sau khi Microsoft phát hành bản v&aac

Tạp chí InformationWeek - một trong số những tạp chí về công nghệ thông tin hàng đầu thế giới – vừa cho công bố danh sách bình chọn 10 khoảnh khắc tồi tệ nhất của ngành bảo mật thế giới. 1. Lỗi bảo mật trong SQL Đúng một tuần sau khi Microsoft phát hành bản vá lỗi bảo mật cho ứng dụng cơ sở dữ liệu máy chủ SQL thì chuyên gia nghiên cứu David Litchfield trình bày những phát hiện riêng của mình tại diễn đàn Black Hat. Sâu "nhà tù" (slammer worm) đã nhanh chóng tiến hành khai thác lỗi bảo mật trong ứng dụng và làm chậm hệ thống mạng Internet trong năm 2003. 2. Lỗi bảo mật trong tính năng "Plug and Play" của Windows Tháng 4/2005, các chuyên gia nghiên cứu bảo mật hệ thống Internet phát hiện lỗi trong tính năng "Plug and Play" của Windows có thể cho phép tin tặc lợi dụng khai thác chiếm quyền điều khiển hoặc thực thi các đoạn mã từ xa trên các hệ thống mắc lỗi. Bốn tháng sau (08/2005) sâu Zotob với khả năng khai thác lỗi bảo mật kể trên đã bùng phát mạnh mẽ. 3. Lỗi tràn bộ nhớ đệm trong Cisco IOS Tháng 07/2005, Michael Lynn - cựu chuyên gia nghiên cứu của ISS – cho biết tin tặc có thể chiếm quyền điểm khiển hệ thống mạng của các doanh nghiệp thông qua một lỗi bảo mật trong phần mềm IOS điều khiển thiết bị định tuyến mạng (router) của Cisco. Đến tháng 4/2006, Cisco mới cho bít lỗ hổng bảo mật này đồng thời kiện Lynn vì đã tiết lộ những thông tin liên quan. Vụ kiện sau đó đã kết thúc mà không có kết quả gì. 4. Lỗi bảo mật định dạng Metafile trong Windows Tháng 01/2006, chuyên gia nghiên cứu H.D. Moore cùng với một số người khác đã tung lên mạng các đoạn mã khai thác lỗi bảo mật trong định dạng tệp tin metafile của Windows. Chuyên gia nghiên cứu Ilfak Guilfanov cũng lập trình thành công đoạn mã khai thác. Đây chính là nguyên nhân khiến cho Microsoft phải tung bản vá lỗi trước lịch trình tới 5 ngày. 5. Lỗi mã hoá dữ liệu trong suốt của Oracle Tháng 01/2006, chuyên gia nghiên cứu Alexander Kornbrust của Red-Database-Security đã chính thức công bố chi tiết về lỗ hổng bảo mật này. Oracle cũng phải nhanh chóng ban hành bản vá ngay sau đó. 6. Lỗi cổng gateway Oracle PLSQL Tháng 01/2006 trước sự có mặt của rất nhiều người tại Diễn đàn Black Hat, Litchfield đã cho công bố một lỗi bảo mật trong cổng gateway Procedural Language extension to SQL (PLSQL) của ứng dụng cơ sở dữ liệu Oracle. Đến nay lỗi này vẫn chưa được khắc phục. 7. Lỗi trong ứng dụng Mac iChat Ngày 13/02/2006, một người dấu tên đã cho công bố trên trang web MacRumors.com một liên kết thông tin về con trojan OSX/Leap.a. Đây được xem là con virus đầu tiên nhắm mục tiêu tấn công hệ điều hành Apple OS X. 8. Lỗi createTextRange() của Internet Explorer Tháng 03/2006, chuyên gia nghiên cứu Andreas Sandblad đã phát hiện ra lỗi bảo mật này trong trình duyệt Internet Explorer của Microsoft. Tin tặc có thể lợi dụng khai thác để cài đặt các phần mềm độc hại như spyware hay keylogger lên hệ thống của người dùng. eEye cùng một số hãng bảo mật khác đã phát hành các bản vá không chính thức cho lỗi bảo mật này. Đến ngày 11/04/2006 Microsoft mới khắc phục lỗi này. 9. Lỗi bảo mật trong định dạng tệp tin HTA của Internet Explorer Chuyên gia nghiên cứu bảo mật người Hà Lan Jeffrey van der Stad, tháng 03 vừa qua, đã cảnh báo Microsoft về lỗi bảo mật liên qua đến cách trình duyệt Internet Explorer xử lý các thẻ HTML. Van der Stad đã loại bỏ các thông tin về lỗi bảo mật này trên trang web của mình khi Microsoft phản ánh về việc công bố công khai này. 10. Lỗi bảo mật trong SendMail SMTP Tháng 03/2006, ISS đã phát hiện ra lỗi bảo mật trong giao thức SMTP của phần mềm máy chủ Sendmail. Nhà phá triển phần mềm đã ngay lập tức phát hành

bản vá lỗi. Hoàng Dung