SUN BÍT LỖ HỔNG NGHIÊM TRỌNG TRONG JAVA

Hôm 08/02, Sun Microsystems đã cho ban hành một bản vá bảo mật nhằm sửa bẩy lỗi nghiêm trọng trong Java Runtime Environment (JRE). Đây là những lỗ hổng bảo mật được xếp vào mức độ "cực kỳ nguy hiểm" vì chúng hoàn toàn có thể bị tin tặc ác

Hôm 08/02, Sun Microsystems đã cho ban hành một bản vá bảo mật nhằm sửa bẩy lỗi nghiêm trọng trong Java Runtime Environment (JRE). Đây là những lỗ hổng bảo mật được xếp vào mức độ "cực kỳ nguy hiểm" vì chúng hoàn toàn có thể bị tin tặc ác ý lợi dụng khai thác nhằm từ xa chiếm quyền kiểm soát hệ thống của người sử dụng. Theo một bản tin khuyến cáo bảo mật của Secunia, bẩy lỗi bảo mật nghiệm trọng ảnh hưởng đến môi trường Java Runtime Environment chạy trên nền tảng các hệ điều hành Windows, Solaris và Linux sử dụng các phiên bản Java Development Kit 1.5, Software Development Kit (SDK) 1.3 và 1.4, JRE 1.3, 1.4, 1.5 và 5.0 hay thấp hơn. Secunia xếp các lỗ hổng bảo mật kể trên vào mức "cực kỳ nguy hiểm". Phần mềm JRE của Sun - đặc biệt là phiên bản 1.4 - được cài đặt rất phổ biến trên các loại máy tính hiện này nhằm tạo môi trường hoạt động cho các ứng dụng Java. Những ứng dụng này vận hành trong một khu vực riêng tách biệt khỏi hệ thống của người sử dụng có tên gọi là "sandbox" Những lỗi bảo mật mới nhất này được phát hiện ra trong một giao diện lập trình ứng dụng JRE hay còn gọi là API – thành phần cho phép tạo sự liên kết trao đổi thông tin giữa các "sandbox" với hệ thống. Những lỗi bảo mật này có thể bị tin tặc khai thác để từ xa truy cập tới các ứng dụng Java của người sử dụng cho phép chúng có thể đọc ghi các tệp tin hay thực thi các đoạn mã. Vào tháng 11 năm ngoái Sun cũng đã phải cho ban hành một bản vá để sửa năm lỗi bảo mật khác trong JRE cũng có liên quan đến các hàm API.