# PHÁT HIỆN LỖ HỔNG NGHIÊM TRỌNG TRONG JAVA RUNTIME ENVIRONMENT

Hãng b

Hãng bảo mật Secunia vừa cảnh báo một lỗ hổng nghiêm trọng trong Sun Java Runtime Environment (JRE), có thể cho phép tin tặc chiếm dụng hệ thống bị ảnh hưởng.

Lỗ hổng phát sinh do một sai sót trong quá trình xử lý ảnh GIF của JRE, và có thể bị khai thác để tấn công tràn bộ đệm "heap" thông qua một file ảnh GIF được tin tặc tạo ra (có độ rộng bằng 0).

Theo cảnh báo, các trường hợp khai thác thành công có thể cho phép thực thi mã nhị phân. Lỗ hổng được xác định ảnh hưởng tới các phiên bản:

* JDK và JRE 5.0 Update 9 và các phiên bản trở về trước.
* SDK và JRE 1.4.2_12 và các phiên bản trở về trước.
* SDK và JRE 1.3.1_18 và các phiên bản trở về trước.

Người dùng có thể sử dụng trình phần mềm Secunia Software Inspector để kiểm tra xem hệ thống có bị ảnh hưởng bởi lỗ hổng trên hay không.

Giải pháp: Nâng cấp lên các phiên bản cao hơn:

+ JDK và JRE 5.0: Nâng cấp lên bản JDK và JRE 5.0 Update 10 hoặc cao hơn: http://java.sun.com/javase/downloads/index_jdk5.jsp
+ SDK và JRE 1.4.x: Nâng cấp lên bản SDK và JRE 1.4.2_13 hoặc cao hơn: http://java.sun.com/j2se/1.4.2/download.html
+ SDK và JRE 1.3.x: Nâng cấp lên bản SDK và JRE 1.3.1_19 hoặc cao hơn: http://java.sun.com/j2se/1.3/download.html