CVE-2013-1571

Oracle Javadoc HTML frame injection vulnerability

1. Introduction

CVE-2013-1571 is vulnerability in Oracle Javadoc HTML pages, which contain a frame injection vulnerability, where you could change a Javadoc web frame with another one. There is some JavaScript code in Javadoc which fails to parse scheme relative URLs parameters correctly.

Oracle Java Development Toolkit lets you generate API documentation in HTML format from comments in the source code.

2. Vulnerability

Someone could change a frame in the web page generated by Javadoc, with another frame which could be harmful. This vulnerability could be used directly for social engineering or phishing.

If you combine it with another browser-related vulnerability you can use it for browser exploitation.

This vulnerability is in Javadoc versions 7 update 21 and before, 6 update 45 and before, 5 update 45 and before, JavaFX 2.2.21 and before.
3. Solution

The vulnerability has been fixed in the June 2013 update of Java. After updating you should regenerate the affected HTML pages and replace them. They also added a fix-in-place tool that will search sub-directories or sub-folders for files named index.htm/html and toc.htm/html. In case of each of those files the tool will find the JavaScript where the vulnerability is at and change it. It will only find the files with the given names, so if you have hanged the name it is smarter to regenerate a new page. This Update makes sure that the generated Javadoc files no longer have JavaScript code which fails to parse scheme relative URLs paramaters correctly. The JavaScript has been changed, unfortunately the code is not available, so I can not add it here.

4. Reference

http://www.oracle.com/technetwork/topics/security/alerts-086861.html
http://www.kb.cert.org/vuls/id/225657