Sun Java JRE Multiple Vulnerabilities
2006-12-20 16:59:13 by Raven

 SECUNIA ADVISORY ID: SA23445

VERIFY ADVISORY: http://secunia.com/advisories/23445/

CRITICAL: Highly critical

IMPACT: Privilege escalation, System access

SOFTWARE:
Sun Java JDK 1.5.x - http://secunia.com/product/4621/
Sun Java JRE 1.5.x / 5.x - http://secunia.com/product/4228/
Sun Java JRE 1.4.x - http://secunia.com/product/784/
Sun Java JRE 1.3.x - http://secunia.com/product/87/
Sun Java SDK 1.4.x - http://secunia.com/product/1661/
Sun Java SDK 1.3.x - http://secunia.com/product/1660/

DESCRIPTION: Some vulnerabilities have been reported in Sun Java JRE (Java Runtime Environment), which can be exploited by malicious people to compromise a user's system.

1) Two errors exist in the Java Runtime Environment, which can be exploited by malicious, untrusted applets to read and write local files, or to execute local applications.

2) Two errors related to serialisation exist in the Java Runtime Environment, which can be exploited by a malicious, untrusted applet to elevate it's privileges.

The following releases are affected:
* JDK and JRE 5.0 Update 7 and prior
* SDK and JRE 1.4.2_12 and prior
* SDK and JRE 1.3.1_18 and prior (not affected by vulnerability #2)

SOLUTION: Update to fixed versions:
JDK and JRE 5.0: Update to JDK and JRE 5.0 Update 8 or later.
http://java.sun.com/javase/downloads/index_jdk5.jsp
SDK and JRE 1.4.x: Update to SDK and JRE 1.4.2_13 or later.
http://java.sun.com/j2se/1.4.2/download.html
SDK and JRE 1.3.x: Update to SDK and JRE 1.3.1_19 or later.
http://java.sun.com/j2se/1.3/download.html

PROVIDED AND/OR DISCOVERED BY:
The vendor credits:
#1) Chris Evans
#2) Tom Hawtin

ORIGINAL ADVISORY:

Sun:

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102729-1

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102731-1

http://scary.beasts.org/security/CESA-2005-008.txt

https://www.ravenphpscripts.com/modules.php?name=News&file=article&sid=2576