

Forum:[Hack Forums](#)

Thread: [Sun Java JRE 1.6.x/6.x Patch](#)

JoshuaXiong - October 13, 2010, 5:38 pm

Download new update: <http://javadl.sun.com/webapps/download/AutoDL?BundleId=42732>

Description

Multiple vulnerabilities have been reported in Sun Java, which can be exploited by malicious users to cause a DoS (Denial of Service) and by malicious people to disclose potentially sensitive information, manipulate certain data, and compromise a vulnerable system.

1) An error in the 2D component may allow execution of arbitrary code.

2) An error in the 2D component may allow execution of arbitrary code.

3) An integer overflow error in the "JPEGImageWriter.writeImage()" function when processing JPEG image dimensions of a subsample can be exploited to corrupt memory.

Successful exploitation may allow execution of arbitrary code.

4) An integer overflow error in the color profile parser when processing the ICC Profile Device Information Tag structure fails to properly allocate memory.

Successful exploitation may allow execution of arbitrary code.

5) An error in the 2D component may allow execution of arbitrary code.

6) An integer overflow error in the color profile parser when processing the ICC Profile Unicode Description Tag structure fails to properly allocate memory.

Successful exploitation may allow execution of arbitrary code.

7) An error in the CORBA component may allow execution of arbitrary code.

8) An error in the com.sun.jnlp.BasicServiceImpl class when retrieving a security policy can be exploited to remove sandbox restrictions.

Successful exploitation may allow execution of arbitrary code.

9) An error in the JRE component may allow execution of arbitrary code.

10) An error in the JRE component may allow execution of arbitrary code.

11) An error in the Java Web Start component may allow execution of arbitrary code.

12) A boundary error in the New Java Plugin (JP2IEXP.dll) when copying the "docbase" applet parameter can be exploited to cause a stack-based buffer overflow.

Successful exploitation may allow execution of arbitrary code.

13) A signedness error in the "HeadspaceSoundbank.nGetName()" function when parsing BANK records can be exploited to cause a buffer overflow using memcpy() via a specially crafted SoundBank file.

Successful exploitation may allow execution of arbitrary code.

14) An error in the Sound component may allow execution of arbitrary code.

15) An error in the Swing component may allow execution of arbitrary code.

16) An error in the ActiveX plugin fails to properly initialize a window handle and may allow execution of arbitrary code.

17) An error in the Java Web Start component may allow execution of arbitrary code.

18) An error in the Deployment Toolkit component may allow execution of arbitrary code.

19) An error in the CORBA component can be exploited to disclose and manipulate certain data.

20) An error in the JSSE TLS/SSL component can be exploited to manipulate certain data.

21) A NULL-pointer dereference error in Kerberos GSS-API can be exploited to cause a DoS.

22) An error in the Networking component can be exploited to disclose and manipulate certain data.

23) An error in the Swing component can be exploited to disclose and manipulate certain data.

24) An error in the Networking component can be exploited to disclose and manipulate certain data.

25) An error in the Networking component can be exploited to disclose and manipulate certain data.

26) An error in the Networking component can be exploited to disclose and manipulate certain data.

27) An error in the JNDI component can be exploited to disclose certain data.

28) An error in the Networking component can be exploited to disclose certain data.

29) An error in the Networking component can be exploited to disclose certain data.

Solution

Apply updates.

Provided and/or discovered by

3) An anonymous person, reported via ZDI.

4,6) Intevydis, reported via ZDI.

8) Matthias Kaiser, reported via ZDI.

12,16) Stephen Fewer of Harmony Security, reported via ZDI.

13) An anonymous person, reported via ZDI.

16) An anonymous person, reported via ZDI.

It is currently unclear who reported these vulnerabilities as the Oracle Critical Patch Update for October 2010 only provides a bundled list of credits. This section will be updated when/if the original reporter provides more information.

-mothered- - *October 13, 2010, 7:10 pm*

Very Interesting documentation mate, that's come as a surprise to me.
Thanks.

Kyuubi - *October 13, 2010, 9:35 pm*

That's a pretty big update, I'll make sure to update ASAP.

Great Prosperity - *October 13, 2010, 10:36 pm*

Yes, its very important to update because the old java versions have a lot of vulnerabilities. :/

MasterMind98 - *October 15, 2010, 10:22 am*

It's good that I always stay updated.