

# [NEWS] Java Web Start Encoding Stack Buffer Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00049.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 16 Mar 2008 13:17:07 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Java Web Start Encoding Stack Buffer Overflow

---

## SUMMARY

A vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Sun Java Web Start. User interaction is required to exploit this vulnerability in that the target must visit a malicious page.

## DETAILS

### Vulnerable Systems:

- \* JDK and JRE 6 Update 4 and earlier
- \* JDK and JRE 5.0 Update 14 and earlier
- \* SDK and JRE 1.4.2\_16 and earlier

### Immune Systems:

- \* JDK and JRE 6 Update 5 or later
- \* JDK and JRE 5.0 Update 15 or later
- \* SDK and JRE 1.4.2\_17 or later

The specific flaw exists in the useEncodingDecl() function used while parsing the xml header character encoding attribute. When a user downloads

## [NEWS] Java Web Start Encoding Stack Buffer Overflow

a malicious JNLP file, the charset value is read into a static buffer. If an overly charset name in the xml header is included, a stack based buffer overflow occurs, resulting in an exploitable condition.

### Vendor Response:

Sun Microsystems has issued an update to correct this vulnerability. More details can be found at:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-233323-1>  
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-233323-1>

### Workaround:

To reduce the likelihood of executing untrusted applications which may allow these issues to be exploited, Java Web Start applications may be disabled temporarily (until the updates or patches have been installed) as follows:

#### For Internet Explorer (Windows):

1. Right click on the "Start" button and select "Explore"
2. In the "Start Menu" window, select "Tools" => "Folder Options"
3. From the "Folder Options" window, select the "File Types" tab
4. From the "Registered File Types" window, scroll down and locate the "JNLP – JNLP File"
5. Select the "JNLP – JNLP File" and click the "Delete" button

#### For Mozilla:

1. Select "Preferences" under the browser's "Edit" menu
2. In the "Preferences" window, select "Helper Applications" located under the "Navigator" category
3. Under "File types", scroll down and locate "application/x-java-jnlp-file"
4. Select "application/x-java-jnlp-file" and click the "Remove" button

Note 1: On Microsoft Windows, applications may also be launched from the desktop icon or Start Menu if a shortcut was previously created for an application. Unknown applications should not be launched through the desktop icon or the Start Menu. Shortcuts can be removed by using the Java Web Start Application Manager through the "Application Remove Shortcut" menu item. For more information, see:

<http://java.sun.com/j2se/1.5.0/docs/guide/javaws/developersguide/overview.html#jws>  
<http://java.sun.com/j2se/1.5.0/docs/guide/javaws/developersguide/overview.html#jws>

Note 2: It is also possible to launch applications through the command line in Windows, Solaris, and Linux. Unknown applications should not be launched through the command line. Sites may consider renaming the Java Web Start launcher ("javaws.exe" for Windows and "javaws" for Solaris and Linux) to prevent Java Web Start from launching.

The launcher can be found at:

[NEWS] Java Web Start Encoding Stack Buffer Overflow

For Windows:

JDK and JRE 6: C:\Program Files\Java\jre1.6.0\_03\bin\javaws.exe

JDK and JRE 5: C:\Program Files\Java\jre1.5.0\_13\bin\javaws.exe

SDK and JRE 1.4.2: C:\Program Files\Java\j2re1.4.2\_16\javaws\javaws.exe

For Solaris (if installed using pkg):

/usr/bin/javaws

For Linux (if installed using rpm):

/usr/java/jre1.5.0/bin/javaws

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1188>>  
CVE-2008-1188

Disclosure Timeline:

2007-09-14 – Vulnerability reported to vendor

2008-03-12 – Coordinated public release of advisory

ADDITIONAL INFORMATION

The information has been provided by <<mailto:zdi-disclosures@xxxxxxxx>>

The Zero Day Initiative (ZDI).

The original article can be found at:

<<http://www.zerodayinitiative.com/advisories/ZDI-08-010>>

<http://www.zerodayinitiative.com/advisories/ZDI-08-010>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.