

[NT] Sun J2RE DoS Issue (RFC2397)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-01/msg00019.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 10 Jan 2008 13:28:41 +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>

Sun J2RE DoS Issue (RFC2397)

SUMMARY

The aim of this document is to clearly define an issue that exists with the Sun JRE product [1] that will allow an attacker to cause the JRE and Internet Explorer to fail, possibly losing unsaved work etc.

DETAILS

Vulnerable Systems:

- * Sun JRE 5.0 prior to update 14

Sun JRE is described [1] as "the Java APIs, Java Virtual Machine (HotSpot VM), and other components necessary to run applets and applications written in the Java programming language".

The software provides a virtualisation layer that allows java applications to be run across platforms and operating systems. These java applications can be delivered to the JVM via a number of mechanisms, and are commonly downloaded from a web server or less commonly, can be embedded within HTML content.

Analysis:

[NT] Sun J2RE DoS Issue (RFC2397)

The RFC2397 [2] standard allows for the encoding of java applets within a URI, allowing it to be embedded in an HTML document.

If an applet is encoded into the data parameter of an object tag with an undefined "name" attribute, and is then passed to Internet Explorer, then when the application is unencoded and passed in turn to the JVM it causes a null pointer exception to occur in jpiexp32.dll.

Recommendations:

Upgrade to a version of the Sun JRE product that does not exhibit this issue (such as Sun JRE 6.0 or JRE 5.0 update 14), and uninstall all effected versions. This is important, as it is possible for an attacker to specify which local VM will be used to run an applet (and so select a vulnerable version).

References:

- [1] <<http://java.sun.com/javase/>> <http://java.sun.com/javase/>
- [2] <<http://www.ietf.org/rfc/rfc2397>> <http://www.ietf.org/rfc/rfc2397>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:martin.oneal@xxxxxxxxxxxxxx>> Martin O'Neal.

=====

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

=====
=====

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.