

# [NEWS] JFreeChart Image Map Cross-Site Scripting Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-12/msg00013.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 9 Dec 2007 11:21:08 +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>

-----

## JFreeChart Image Map Cross-Site Scripting Vulnerabilities

---

### SUMMARY

<<http://sourceforge.net/projects/jfreechart/>> JFreeChart is "a popular Java-based chart library used to generate charts and graphs of data. The library includes support for generating HTML image maps, which allow for enhanced interaction of the chart via hyperlinks bound to shapes specified by coordinates".

Multiple cross-site scripting vulnerabilities exist within the image map support functionality of JFreeChart which may allow an attacker to inject arbitrary HTML or JavaScript into any product or website which uses the library.

### DETAILS

Vulnerable Systems:

- \* JFreeChart version 1.0.8

Immune Systems:

- \* JFreeChart version 1.0.8 branch "jfreechart-1.0.8-security"

## [NEWS] JFreeChart Image Map Cross-Site Scripting Vulnerabilities

JFreeChart fails to properly escape the following properties of the generated image map:

- \* The chart name.
- \* The chart tool tip text.
- \* The href attribute for a chart area.
- \* The shape attribute for a chart area.
- \* The coords attribute for a chart area.

It is possible to inject custom HTML code into the code generated by the JFreeChart library. If a web server uses this library to generate charts from user-supplied data, an attacker could cause other users of the same website or application to execute arbitrary JavaScript code when viewing a page containing a chart.

Vendor status and information:

The JFreeChart project was notified of this vulnerability on November 28th, 2007 via their online bug tracking system. The vulnerability was fixed on December 6th 2007 with a commit to their SVN repository.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:advisory@xxxxxxxxxx>> Rapid7 Advisory.

The original article can be found at:

<<http://www.rapid7.com/advisories/R7-0031.jsp>>  
<http://www.rapid7.com/advisories/R7-0031.jsp>

=====

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](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto: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.