

# New Macromedia Security Zone Bulletin Posted

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-05/0107.html>

---

**From:** Macromedia Security Zone ([securityzone\\_at\\_macromedia.com](mailto:securityzone_at_macromedia.com))

**Date:** 05/10/05

Date: Tue, 10 May 2005 12:03:38 -0700 (PDT)

To: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)

~~~~~  
**IMPORTANT:**

A new security bulletin describes a configuration problem that may affect ColdFusion installations.

To learn about this new issue and what actions you can take to address it, please visit the Macromedia Security Zone:

<http://www.macromedia.com/go/mpsb05-03>  
~~~~~

**MPSB05-03**

ColdFusion MX 7 cross-site scripting in default error page

Originally posted: May 10, 2005

~~~~~  
**SUMMARY**

The default error page in the optional-use JRun Web Server bundled with ColdFusion MX 7 is vulnerable to a cross-site scripting attack.

~~~~~  
**SOLUTION**

Define a custom error page or download and install the patch referenced below or use an alternative Web Server with ColdFusion.

## SecurityFocus Bugtraq: New Macromedia Security Zone Bulletin Posted

### Affected Software Versions

ColdFusion MX 7.0

~~~~~

### Severity Rating

Macromedia categorizes this issue as a moderate update and recommends users patch their installations immediately.

~~~~~

### Details

A specially encoded URL can be used to create a cross-site scripting attack through the default 404 error page. Exploitation of the vulnerability requires a user to follow a hyperlink to a page that doesn't exist on the server.

Most customers using ColdFusion MX 7 will not be affected by this vulnerability because the majority of customers run ColdFusion MX 7 with other web servers. This vulnerability does not affect ColdFusion servers using connectors to any other web server such as IIS or Apache. Although the JRun Web Server is included with ColdFusion MX 7, it is not recommended for use in production environments and is intended for configuration, evaluation and testing purposes only.

~~~~~

### Making the Changes

NOTE: Back up your existing files before making changes. As always, test the changes in a non-production environment before applying the changes to production servers.

Install the security patch from the ColdFusion MX 7 Administrator. The installation process is the same for all platforms and installation choices.

1. Download chf70-60112.jar (2K).
2. Open the ColdFusion MX 7 Administrator and select the System Information page.
3. Next to the Update File field, select the Browse Button and browse to the downloaded file.
4. Select the file and click Submit.

5. Restart ColdFusion.

The ColdFusion MX 7 hot fix JAR file does not need to be retained after installing it with the ColdFusion Administrator. The file has been copied into the correct location.

The ColdFusion MX 7 hot fix JAR file will appear in the System Information list.

~~~~~  
Reporting Security Issues  
~~~~~

Macromedia is committed to addressing security issues and providing customers with the information on how they can protect themselves. If you identify what you believe may be a security issue with a Macromedia product, please send an e-mail to [secure@macromedia.com](mailto:secure@macromedia.com). We will work to address and communicate the issue appropriately.

~~~~~

Receiving Security Bulletins

When Macromedia becomes aware of a security issue that we believe significantly affects our products or customers, we will notify customers when appropriate. Typically this notification will be in the form of a security bulletin explaining the issue and the response. Macromedia customers who would like to receive notification of new security bulletins when they are released can sign up for our security notification service.

For additional information on security issues at Macromedia, please visit:

<http://www.macromedia.com/security>

~~~~~

ANY INFORMATION, PATCHES, DOWNLOADS, WORKAROUNDS OR FIXES PROVIDED BY MACROMEDIA IN THIS BULLETIN ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MACROMEDIA AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED OR OTHERWISE, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ALSO, THERE IS NO WARRANTY OF NON-INFRINGEMENT, TITLE OR QUIET ENJOYMENT. (USA ONLY) SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU.

IN NO EVENT SHALL MACROMEDIA, INC. OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING, WITHOUT LIMITATION, DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE, COVER, LOSS OF PROFITS, BUSINESS INTERRUPTION OR THE LIKE, OR LOSS OF BUSINESS DAMAGES, BASED ON ANY THEORY OF LIABILITY INCLUDING BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF MACROMEDIA, INC. OR ITS SUPPLIERS OR THEIR REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (USA ONLY) SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU AND YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM STATE TO STATE.

Macromedia reserves the right, from time to time, to update the information in this document with current information.

~~~~~  
Macromedia Support, Privacy, and Unsubscribe Information  
~~~~~

Macromedia Support:  
<http://www.macromedia.com/support/>

Macromedia and your privacy:  
<http://www.macromedia.com/help/privacy.html>

Contact Macromedia:  
Thank you for your continued interest in Macromedia products. If you'd rather not receive updates about events, classes, or products, write to [newsflash@hvm.macromedia.com](mailto:newsflash@hvm.macromedia.com) and type "no thanks" in the Subject line. You may also change your communication preferences by visiting this web page:

<http://www.macromedia.com/go/unsubupdates?email=bugtraq@securityfocus.com>

Macromedia, 601 Townsend St., San Francisco, California 94103