

# [securityzone@macromedia.com: New Macromedia Security Zone Bulletin Posted]

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-04/0034.html>

---

**From:** David Ahmad (*da\_at\_securityfocus.com*)

**Date:** 04/03/04

Date: Sat, 3 Apr 2004 13:35:05 -0700

To: bugtraq@securityfocus.com

----- Forwarded message from Macromedia Security Zone <securityzone@macromedia.com> -----

From: securityzone@macromedia.com (Macromedia Security Zone)  
Subject: New Macromedia Security Zone Bulletin Posted  
Reply-To: securityzone@macromedia.com (Macromedia Security Zone)  
Date: Fri, 2 Apr 2004 14:40:08 -0800 (PST)  
X-Mailer: Protagona email services (Version 5.50.1620)  
Message-Id: <200404022240.i32McaNd025075@hvm02.macromedia.com>

~~~~~  
Security Bulletin

MPSB 04-05 Potential Risk in Dreamweaver Remote Database Connectivity

Originally posted: April 1, 2004

Last updated: April 1, 2004  
~~~~~

Summary:

Dreamweaver's remote database connectivity for testing dynamic database-driven websites installs scripts that may reveal DSNs to outside attackers. A sophisticated attacker may also be able to use these scripts to send SQL commands to the server and gain control of the database server.

~~~~~  
Solution:

Customers should not define a database connection using the driver on a testing server accessible to the public. To prevent unauthorized access to the database, password-

protect the database. If a database connection has been defined, use Dreamweaver's Remove Connection Scripts menu command to remove the files that expose the database. This issue is described in greater detail in Security implications of remote database connectivity (TechNote 19214).

[http://www.macromedia.com/go/DMJL\\_AACE](http://www.macromedia.com/go/DMJL_AACE)

~~~~~

#### Severity Rating:

Macromedia categorizes this issue as a critical update and recommends affected users immediately remove the connection scripts from publicly accessible servers.

[http://www.macromedia.com/go/DMJL\\_AACF](http://www.macromedia.com/go/DMJL_AACF)

~~~~~

#### Affected Software Versions:

Dreamweaver MX 2004 (all versions)  
Dreamweaver MX (all versions)  
Dreamweaver UltraDev 4 (all versions)

~~~~~

#### Details:

When you specify "Using Driver On Testing Server" or "Using DSN on Testing Server" in the database connections dialog box, Dreamweaver automatically uploads a script file to the testing server that allows Dreamweaver to manipulate the remote database driver via the HTTP protocol. This allows Dreamweaver to get the database information it needs in order to help the user create their site. However, this file does make it possible to see the data source names (DSNs) defined on the system. If the DSNs and databases are not password protected, the script also enables an attacker to issue SQL commands to the database.

~~~~~

#### Acknowledgements:

Macromedia would like to thank David Litchfield of Next Generation Security Software Limited for reporting this

vulnerability and for working with us to help protect our customers' security.

~~~~~

Revisions:

April 1, 2004, bulletin first created.

~~~~~

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 appropriately address and communicate the issue.

~~~~~

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:

Macromedia, 600 Townsend St., San Francisco, California 94103

----- End forwarded message -----

--

David Mirza Ahmad  
Symantec

PGP: 0x26005712

8D 9A B1 33 82 3D B3 D0 40 EB AB F0 1E 67 C6 1A 26 00 57 12