

[NEWS] Macromedia JRun Admin Server Authentication Bypass

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0003.html>

From: support@securiteam.com

Date: 07/01/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 1 Jul 2002 07:35:05 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Macromedia JRun Admin Server Authentication Bypass

SUMMARY

JRun is Macromedia's servlet / JSP engine. It installs a web based administration console on TCP port 8000. Before the console can be used by users, they are required to login via an HTML form. This form can be bypassed and administrative functions accessed without authentication.

DETAILS

Vulnerable systems:

- * JRun versions 3.0/3.1/4.0 (Without the patch)

Immune systems:

- * JRun versions 3.0/3.1/4.0 (With the patch)

The login form is the default page served up by the server on port 8000. By inserting an extra '/' in the URL we bypass the login form and gain access to the web based admin console, e.g.:

<http://JRun-Server/>

We do not have unrestricted access to the admin console – clicking on further links returns you to the login page. However, by requesting the

Securiteam: [NEWS] Macromedia JRun Admin Server Authentication Bypass

desired admin function in the initial URL we bypass this restriction also,
e.g.:

JRun-Server:8000/welcome.jsp?&action=stop&server=default

Will shutdown the 'default' JRun server instance on port 8100. Other administrative functions can also be accessed.

Patch Information:

Macromedia have produced a cumulative patch for JRun 3.0/3.1/4.0, availability of which is described in the bulletin at:

<<http://www.macromedia.com/v1/handlers/index.cfm?ID=23164>>
<http://www.macromedia.com/v1/handlers/index.cfm?ID=23164>

ADDITIONAL INFORMATION

The information has been provided by <mailto:matt@westpoint.ltd.uk> Matt Moore.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] Simple WAIS Allows Users to Execute Commands as the SWAIS Daemon."
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)