

[NEWS] Macromedia JRun Web Server URL Parsing Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00077.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 22 Dec 2005 12:31:24 +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>

Macromedia JRun Web Server URL Parsing Buffer Overflow

SUMMARY

" <<http://www.macromedia.com/software/jrun/>> Macromedia JRun 4 is an application server used for developing and deploying Java based applications."

Remote exploitation of a buffer overflow vulnerability in Macromedia JRun 4 allows attackers to execute arbitrary code or cause a denial of service condition.

DETAILS

Vulnerable Systems:

- * Macromedia JRun 4 prior to Updater 5

Immune Systems:

- * Macromedia Run 4 Updater 5
- * Macromedia Run 4 Updater 6

The vulnerability exists within the JRun web server, specifically in the handling of long request strings. In certain configurations, when a long

[NEWS] Macromedia JRun Web Server URL Parsing Buffer Overflow

(approximately 64k) URL is supplied, a stack-based overflow occurs potentially allowing the execution of arbitrary code. In testing performed it was possible to overwrite the saved return address on the stack with remotely supplied values (converted into 'wide characters' by the server).

Successful exploitation allow remote attackers to execute arbitrary code with Local System privileges. The supplied JRun web server must be active for the attack vector to exist. It is not recommended to use the JRun web server component in production systems, as the installer mentions that it should be used for development only.

As the service restarts after each crash, it is possible to make multiple attempts to exploit this issue, and each time restart from a 'clean' state.

Although this vulnerability allows a stack overwrite, it may be more difficult to exploit due the input string being converted into a 'wide character' version of the str input, by placing a null byte between each character. While this does not necessarily prevent exploitation, it does increase the complexity of developing an exploit.

Exploitation of this vulnerability may allow a remote attackers to execute code on the affected system as Local System, allowing complete compromise, or cause a denial of service against the affected system, preventing legitimate use.

Workaround:

The JRun documentation suggests that the JRun Web Server should not be used in a production environment. In a development environment, the JRun server should not accept connections from outside of the development network.

Disclosure Timeline:

08/25/2004 – Initial vendor notification
08/31/2004 – Initial vendor response
12/21/2005 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@xxxxxxxxxxxxxxxxxxxxx>> iDEFENSE Labs .

The original article can be found at:

<<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=360>>
<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=360>

The vendor advisory can be found at:

<http://www.macromedia.com/devnet/security/security_zone/mpsb05-13.html>
http://www.macromedia.com/devnet/security/security_zone/mpsb05-13.html

=====
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

In order to subscribe to the mailing list, simply forward this email to: 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.

-
- Prev by Date: [***\[NT\] FTGate Multiple Vulnerabilities \(LIST, AUTHENTICATE, USER, PASS, TOP, tzoffset\)***](#)
 - Next by Date: [***\[TOOL\] Synner – Spoof-DoS Tool***](#)
 - Previous by thread: [***\[NT\] FTGate Multiple Vulnerabilities \(LIST, AUTHENTICATE, USER, PASS, TOP, tzoffset\)***](#)
 - Next by thread: [***\[TOOL\] Synner – Spoof-DoS Tool***](#)
 - Index(es):
 - ◆ [***Date***](#)
 - ◆ [***Thread***](#)