

# [NT] Macromedia ColdFusion/JRun Remote SYSTEM Buffer Overflow Vulnerabilities

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0032.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 11/14/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 14 Nov 2002 15:49:10 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

Macromedia ColdFusion/JRun Remote SYSTEM Buffer Overflow Vulnerabilities

---

## SUMMARY

Macromedia JRun and ColdFusion IIS ISAPI handlers contain various heap overflows when handling URI filenames. By supplying a filename over 4096 bytes in size, heap memory can be overwritten. Various structures can be overwritten in the process heap to gain control of the remote IIS process with SYSTEM level access. This makes it rather trivial for attackers to remotely compromise Microsoft IIS web servers running vulnerable versions of Macromedia ColdFusion or JRun.

## DETAILS

Vulnerable systems:

- \* Macromedia ColdFusion 6.0 and prior (IIS ISAPI)
- \* Macromedia JRun 4.0 and prior (IIS ISAPI)

Exploit:

The following requests can be used to duplicate the attack.

For JRun:

```
telnet example.com 80
```

```
GET /[+4096 byte buffer].jsp HTTP/1.0
```

Securiteam: [NT] Macromedia ColdFusion/JRun Remote SYSTEM Buffer Overflow Vulnerabilities

[enter]  
[enter]

For Coldfusion:  
telnet example.com 80  
GET /[+4096 byte buffer].cfm HTTP/1.0  
[enter]  
[enter]

During testing, 5000 bytes was sufficient to begin overwriting data structures that made exploitation straightforward. The vulnerabilities exist in error handling within the ISAPI filters.

Vendor Status:  
Macromedia has released patches for both the JRun and ColdFusion products.  
ColdFusion MX Advisory:  
<<http://www.macromedia.com/v1/handlers/index.cfm?ID=23161>>  
<http://www.macromedia.com/v1/handlers/index.cfm?ID=23161>

JRun Advisory:  
<<http://www.macromedia.com/v1/handlers/index.cfm?ID=23500>>  
<http://www.macromedia.com/v1/handlers/index.cfm?ID=23500>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:marc@eeye.com>> Marc Maiffret of eEYE.

=====

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](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[NEWS] Remote Novell Netware Manager Security Issue"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)