

# [NT] Patch Available for Default Missing Template page in ColdFusion MX

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0083.html>

---

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

*Date:* 06/19/02

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

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

Date: Wed, 19 Jun 2002 08:46:51 +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.

-----

Patch Available for Default Missing Template page in ColdFusion MX

---

## SUMMARY

The default Missing Template handler in ColdFusion MX displays the missing template URI without checking the filename for invalid characters. This may allow a filename to contain executable JavaScript strings. This vulnerability is also sometimes called "Cross Site Scripting".

## DETAILS

Vulnerable systems:

\* ColdFusion MX (English release, All Editions, All Platforms)

Macromedia's ColdFusion MX comes with a default 404 error page. This 404 error page presents the path of the file requested, and does not filter it for hazardous characters, which might be used for a cross site scripting attack. For example, the following requests will pop-up a message containing the current session cookies:

[http://CF\\_MX\\_SERVER/>alert\(document.cookie\)</script>.cfm](http://CF_MX_SERVER/>alert(document.cookie)</script>.cfm)

Solution:

Customers should either:

1) Create their own Missing Template Handler and specify this handler in

Securiteam: [NT] Patch Available for Default Missing Template page in ColdFusion MX

the Settings page of ColdFusion Administrator. This handler should not display the missing URI

2) Install the patch. The patch consists of a replacement template which can be downloaded from

<[http://download.macromedia.com/pub/security\\_zone/cfm/MPSB02-03.zip](http://download.macromedia.com/pub/security_zone/cfm/MPSB02-03.zip)>

MPSB02-03: Security Update. This file is a replacement for:

\* Windows:

{installation\_directory}\CFusionMX\wwwroot\WEB-INF\exception\detail.cfm

\* Unix:

{installation\_directory}/CFusionMX/wwwroot/WEB-INF/exception/detail.cfm

ADDITIONAL INFORMATION

The information has been provided by <mailto:[ORY.SEGAL@SANCTUMINC.COM](mailto:ORY.SEGAL@SANCTUMINC.COM)>  
Ory Segal.

=====

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): "[TOOL] Systrace – Interactive Policy Generation for System Calls"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)