

[NEWS] ColdFusion Cross-Site Scripting Security Vulnerability (Default Error Page)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0085.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/24/03

To: list@securiteam.com

Date: 24 Sep 2003 11:14:41 +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>

ColdFusion Cross-Site Scripting Security Vulnerability (Default Error Page)

SUMMARY

ColdFusionMX Web Sites that use the default ColdFusionMX Site-Wide Error Handler page or the default ColdFusionMX Missing Template Handler page may be susceptible to a cross-site scripting attack using the HTTP Referer[sic] header field.

DETAILS

Affected Software Versions:

- * ColdFusion MX 6.0 and 6.1 (All editions)
- * ColdFusion MX 6.0 J2EE (All editions)
- * ColdFusion MX 6.1 J2EE (All editions)
- * ColdFusion 5.0 and prior versions

Technical details:

In the default error page, two ColdFusion tags are showed #error.HTTPReferer# and #error.QueryString#, both these tags are not filtered for arbitrary HTML or JavaScript code. This allows attackers to cause the web site to return third-party content (content sent by an

Securiteam: [NEWS] ColdFusion Cross-Site Scripting Security Vulnerability (Default Error Page attacker).

Solution:

A patch corresponding to this problem can be found at:

<http://www.macromedia.com/devnet/security/security_zone/mpsb03-06.html>
http://www.macromedia.com/devnet/security/security_zone/mpsb03-06.html.

ADDITIONAL INFORMATION

The information has been provided by <mailto:pfh00062@nifty.com> T.Hara of Vagabond and <mailto:robertfly@hotmail.com> Robert Fly.

=====

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.