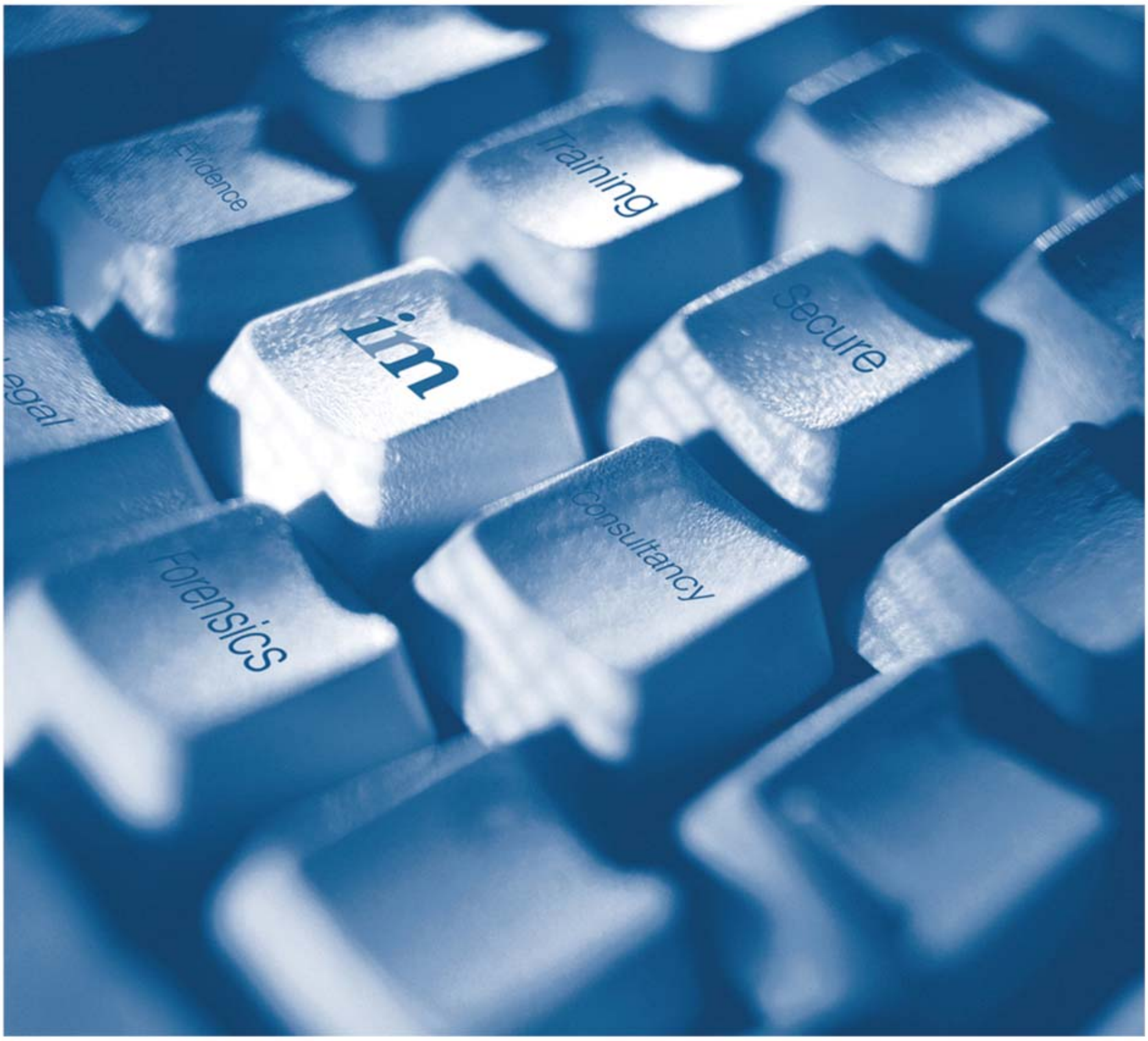
InformationRiskManagement

Product Security Briefing

Performed on:

Adobe ColdFusion 8



Information Risk Management Plc 8th Floor Kings Building Smith Square London SW1P 3JJ
Tel: +44 (0)20 7808 6420 Fax: +44 (0)20 7808 6421 info@irmplc.com http://www.irmplc.com

ColdFusion 8

ColdFusion 8 allows developers to quickly and easily create compelling Internet applications that fit in today's complex enterprise environments. On completion of a comprehensive application security review, IRM ascertained that ColdFusion 8 exhibits a high degree of resilience to application layer attacks with no compromise on functionality provisioned by the new features.

Overview

IRM's static source code analysis, coupled with creative scenario-based testing techniques, revealed the security best practices that have been adopted during the development of ColdFusion 8. While application controls were subjected to rigorous testing and malicious input, all of them fared extremely well in countering threats posed to the application architecture. ColdFusion 8 provisions a platform for developers whereby they can focus on delivering feature-rich Internet applications with the knowledge that the product has been developed with security in mind. This document details various new components within ColdFusion 8 and corresponding security controls which mitigate security threats to them.

New Features Overview

A range of new features have been added to ColdFusion in this latest version; these include:

- New Authentication and Authorisation model
- Multi Server monitoring
- A new Eclipse plug-in debugger
- AJAX features
- More than 50 new CFML tags and functions.
- .NET Integration

New Authentication and Authorisation model

One of the obvious changes in ColdFusion 8 is the way users authenticate to the administration interface. In previous versions only a single administrative user existed; however, now multiple users can be configured, each of which are associated with a list of roles. This major change in a security component required rigorous, systematic testing in order to ensure that there was no negative impact on the security of the product as a result of its implementation. IRM were able to confirm that the introduction of users and roles into the ColdFusion security model not only had been correctly implemented, but also raised the overall security of the product.

Server Monitoring

A server monitoring feature has been implemented, which facilitates real time actionable information on the status of a ColdFusion deployment or multiple deployments via a single interface. This is useful for developers who need to analyse problems during various development phases and administrators who need to monitor health of their servers. Such functionality has its own security requirements which need to be enforced in order to ensure that information provisioned by this feature is made available only to legitimate entities. For example, the authentication credentials associated with each ColdFusion server to monitor need to be securely stored and managed. IRM not only tested the monitoring feature but also examined the cryptographic techniques used to store the authentication credentials and discovered that industry standard cryptographic algorithms had been correctly implemented to adequately protect this sensitive data.

The server monitoring functionality has been implemented as a Flex component, thereby automatically inheriting the security and robustness of a proven technology such as Flex which has been subjected to scrutiny in the past. The monitoring implementation segregates user interfaces from the underlying system which ensures malicious users cannot access protected resources via this feature, thereby reiterating the fact that security was fundamental to the thought process responsible for its design and development.

IRM observed that the new monitoring functionality has been well designed, with security in mind. The implementation adhered to Adobe's security principles for development ensuring that the resultant product exceeded industry standards in terms of security.

Remote Debugging Functionality

The ability to dynamically debug code is central to all application development activities and Adobe has provisioned a way for ColdFusion developers to remotely debug using ColdFusion 8. The debugging functionality allows developers to step through lines of code, inspect variables, observe the code stack etc. As with any other product, enabling remote debugging changes the dynamics of security and requires implementation of countermeasures to prevent the service from being exploited by malicious users.

In order to meet these challenges, ColdFusion remote debugging relies on RDS (Remote Development Services) thereby leveraging security features provisioned by this tried and tested protocol. In order to remotely debug an application, debugging needs to be enabled on the server and RDS authentication credentials are required. IRM subjected this functionality to rigorous testing, evaluating scenarios which involved bypassing the authentication routines of RDS, enabling debugging remotely if it has been disabled etc. In all instances the debugging features performed consistently. However, in line with Adobe's best practices, IRM recommends that debugging should be disabled on all production and Internet-facing servers.

AJAX Features

The AJAX (Asynchronous JavaScript and XML) web development technique enables more interactive applications to be created and ColdFusion 8's implementation provisions a platform which makes the user experience more enriching. AJAX introduces several potential security issues which can be attacked in new creative ways and also increases the likelihood of client side attacks in poor implementations. However, Adobe is aware of these attacks and has mitigated the risks associated with their exploitation.

New CFML Tags

The utilisation of CFML tags has been one of the key factors that allow developers to rapidly create applications with ColdFusion. ColdFusion 8 comprises of a set of new CFML tags which enable developers to manipulate images with a greater degree of control. Each of the new tags, including the image manipulation tags, were subjected to various security test cases to ensure they handled image formats and data correctly and also adhered to ColdFusion's security sandbox model.

Similar to CFML tags previously tested, the new set of tags performed consistently and appropriately to all malformed data supplied. This reaffirms the fact that the security model applicable to other CFML tags has been correctly applied to candidates in the new release. Users can customise the level of resource access each of these tags can have by utilising the sandbox functionality.

.NET Integration

ColdFusion 8 provides native support for .NET objects to integrate ColdFusion applications with enterprise data and infrastructure services. New functionality has been added to ColdFusion 8 to enable .NET assemblies to be called from within ColdFusion applications. The security of this product was rigorously assessed from a "black box" perspective and proved robust to the range of attacks mounted against it.

Exception Handling

In spite of being subjected to non-standard or malformed input, the error handling capabilities of ColdFusion 8 was extremely robust. The product review revealed that extensive use of exception handling resulted in errors being correctly trapped by all of the components.

Industry Standards

In respect to code level security, the source code was well written and adhered to Sun Microsystems guidelines for writing secure code. The robustness of input validation, session management and request handlers negated the possibility of several application layer attacks like command injection, cross site scripting and man in the middle attacks. Apart from this the development platform, in this case J2EE, provides inherent protection from memory corruption vulnerabilities such as buffer overflows.

Conclusion

IRM's security evaluation of ColdFusion 8 revealed that the product has been well designed with security as a major consideration during development. The ColdFusion 8 model requires certain administrative tasks to be performed as a part of deployment in order to enforce a stringent security regime. Security management of these servers is essential in ensuring security of the overall deployment. It is important to follow Adobe's best practice guides for securing these servers and applying appropriate security patches. Adobe also maintains resources on secure development of ColdFusion applications which can be found at the following URL:

http://www.adobe.com/devnet/coldfusion/security.html.

ColdFusion developers should strive to incorporate secure coding principles into their development methodologies as highlighted by Adobe.

Overall IRM was impressed with Adobe's integration of security processes in the development lifecycle, the result of which can be seen in ColdFusion 8, a product that withstands stringent security testing with relative ease. All of the new features incorporated in this release adhere to highest levels of application security enforcement without any compromise on functionality.

About IRM

Information Risk Management Plc (IRM) is a vendor independent information risk consultancy, founded in 1998. IRM has become a leader in client side risk assessment, technical level auditing and in the research and development of security vulnerabilities and tools. IRM is headquartered in London with Technical Centres in Europe and Asia as well as Regional Offices in the Far East and North America. Please visit our website at www.irmplc.com for further information.