Adobe ColdFusion

Secure Profile Web Application Penetration Test

July 31, 2014

Neohapsis
217 North Jefferson Street, Suite 200
Chicago, IL 60661

CONTENTS

1. Executive Summary

At the request of Adobe Systems, Inc. (Adobe), Neohapsis performed a whitebox application assessment of the ColdFusion Splendor Beta application Secure Profile access controls. A whitebox application assessment is a type of "ethical hacking" or "intrusion testing" approach for detecting computer system vulnerabilities that malicious parties could use to exploit a system and compromise its data. It is performed with the cooperation and assistance of the application owner and access to source code and system architecture documents are provided. The goal of the penetration test is to determine if, and to what degree, Adobe customer's network assets could be breached if the application Secure Profile controls were to be circumvented. The assessment took place between February 10 and February 28, 2014 and was conducted remotely from Neohapsis offices.

Neohapsis identified four configuration related vulnerabilities with 'low severity' during the whitebox application assessment. Neohapsis did not identify any vulnerabilities in the secure profile or Secure & Production profile in ColdFusion 11 during the whitebox application assessment. Four configuration related vulnerability with 'low severity' were identified in the developer profile.

The test environment was under Neohapsis control so user accounts were provisioned as necessary. Source code access was also provided via Adobe network access.

Neohapsis recommended addressing the vulnerabilities as soon as possible.

2. Engagement Overview

Founded in 1997, Neohapsis is a trusted provider of consulting services and products that address the information security needs of global enterprises and government agencies. Our heritage of providing expert security consulting and IT risk management services, combined with advanced research and risk management tools from the Neohapsis Labs, enables Neohapsis to solve the complex security problems that are inherent in emerging technologies.

2.1. Scope

Access to source code for ColdFusion was provided in order to assist consultants in verifying and vetting application vulnerabilities. Access to the source for the application was only accessible through the Adobe network.

The purpose of this test was to determine whether, and to what degree, the ColdFusion Splendor Beta application was vulnerable to attack in its current state. A particular emphasis was placed on testing the application after it had been configured to use a “Secure Profile” upon initial deployment. The Neohapsis consultants primarily focused the assessment on the following areas of concern:

- General application architecture issues
- SQL injection
- Cross-site scripting (XSS)
- Session management vulnerabilities
- Insufficient or ineffective authentication and access control
- Server path manipulation and traversal (files, directories, etc.)
- Insufficient or ineffective use of encryption
- Application related denial of service
- Sensitive information exposure
- Platform (public vulnerabilities) and configuration vulnerabilities
- Any applicable issues not explicitly identified above, but covered by pertinent standards (OWASP Top 10, SANS Top 20)

2.2 Methodology

Neohapsis performed a whitebox web application assessment including the following components:

- Spidering - attempts to identify application functionality by automated traversal of site hierarchy and permuting common variations on popular naming conventions
- Manual fault injection - manual submission of malicious data to identify security vulnerabilities in request path
- Automated fault injection (fuzzing) - automated submission of a range of malicious data to identify security vulnerabilities in request path
- Known vulnerability testing - identification of vulnerabilities in the hosting platform (web server, servlet container, etc.) using primarily automated analysis techniques
- Source code review to reveal coding deficiencies and potential areas for investigation
- Access to application design documents
- Access to application owners and experts
- Data correlation
- Research vulnerabilities
- Eliminate false positives
- Investigate the extent of the finding

3. Summary

Neohapsis has provided remediation recommendations and guidance for all findings, for review and action by Adobe ColdFusion. No noteworthy findings were found on a ColdFusion server with secure profile enabled. Please contact Adobe for their internal policy about how they deal with security issues found during these types of engagements.

3.1. Notes of Qualification

1. The degree of assurance provided by any assessment is contingent on:

   (i) The integrity of information provided by the organization during the assessment process;

   (ii) The organization's willingness to allocate the resources necessary to execute a level and scope of assessment appropriate to the security characteristics of the application and the sensitivity of information assets in that environment;

   (iii) The organization's execution of recommended remediation measures.

2. No methodology definitively proves the absence of vulnerabilities.

3. Following assessment and remediation, modifications to an application, its platform, network environment, and new threat vectors may result in new security vulnerabilities.

3.2.

Chicago, Illinois
217 North Jefferson Street, Suite 200
Chicago, IL 60661

Dallas, Texas
15305 Dallas Parkway, Suite 300
Addison, TX 75001