EXECUTIVE REPORT

ADOBE SYSTEMS, INC.

COLDFUSION SECURITY ASSESSMENT

FEBRUARY 18, 2016

BISHOP FOX

This engagement was performed in accordance with the Statement of Work, and the procedures were limited to those described in that agreement. The findings and recommendations resulting from the assessment are provided in the attached report. Given the time-boxed scope of this assessment and its reliance on client-provided information, the findings in this report should not be taken as a comprehensive listing of all security issues.

This report is intended solely for the information and use of Adobe Systems, Inc.

Bishop Fox Contact Information:
+1 (480) 621-8967
contact@bishopfox.com
8240 S. Kyrene Road
Suite A-113
Tempe, AZ 85284

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Project Overview

Adobe Systems, Inc. engaged Bishop Fox to assess the security of the ColdFusion (2016 release) and API Manager applications. The following report details the findings identified during the course of the engagement, which started on November 23, 2015.

Goals

- Understand the ColdFusion (2016 release) and API Manager applications' security posture
- Identify as many security issues as possible in the designated time and scope
- Identify and plan to manage previously unknown risks
- Comply with a customer's request for a third-party security assessment

Approach

The Bishop Fox team conducted a thorough Hybrid Application Assessment the ColdFusion (2016 release) and API Manager applications. The assessment activities included, but were not limited to:

- Automated static code analysis
- Manual penetration testing
- Candidate-point source code review
- Assessment of auxiliary installed services for best practices

Finding Counts

2 Critical
5 High
5 Medium
0 Low
0 Informational

12 Total findings

Remediation

12 Total findings fixed

Scope

ColdFusion (2016 release) (build 297727)

ColdFusion API Manager (build 297727)

Dates

11/23/2015
Kickoff

11/23/2015 – 12/29/2015
Active testing

02/18/2016
Report delivery

Summary of Findings

In aggregate, the ColdFusion (2016 release) and API Manager applications meet their security objectives.

Seven high- and critical-risk vulnerabilities were identified during the assessment. The ColdFusion development team made significant efforts to remediate the findings or otherwise mitigate the issues. **After remediation testing, the Bishop Fox team verified that all findings had been remediated or sufficiently mitigated.**

Detailed List of Findings

The following tables outline the engagement findings and their remediation status.

Activity	Identified Vulnerabilities	Fixed Vulnerabilities
Hybrid Application Assessment	12	12

Remediated findings

Please refer to the Appendix for explanations of finding severity ratings.

CRITICAL SEVERITY

Activity	Finding ID	Vulnerability	Identified	Fixed
Hybrid Application Assessment	1	Cross-site Request Forgery	1	1
	2	XML External Entity (XXE)	1	1

HIGH SEVERITY

Activity	Finding ID	Vulnerability	Identified	Fixed
Hybrid Application Assessment	3	Insecure File Upload	1	1
	4	Server-side Request Forgery	1	1
	5	Arbitrary Remote Code Execution	1	1
	6	Insecure Default Configurations	5	5
	7	Sensitive Information Disclosure	3	3

	Activity	Finding ID	Vulnerability	Identified	Fixed
MEDIUM SEVERITY	Hybrid Application Assessment	8	Insufficient Anti-Automation	2	2
		9	User Interface Redress	1	1
		10	Weak Password Complexity Requirements	4	4
		11	Vulnerable Software	2	2
		12	Ineffective Access Controls	1	1

Recommendations

The Bishop Fox team performed remediation testing and noted that all issues have been successfully remediated or otherwise mitigated. Following the tactical steps in the next section will further reduce the attack surface of the ColdFusion (2016 release) and API Manager applications.

TACTICAL NEXT STEPS

- **Increase Client Security Awareness:** Improve visibility of the ColdFusion security lockdown guides. These guides include a wealth of information to help customers improve the security baseline of their ColdFusion deployments.

APPENDIX A – MEASUREMENT SCALES

The Bishop Fox team used the following criteria to rate the findings in this report.

Finding Severity

The severity of each finding in this report is independent. Finding severity ratings combine direct technical and business impact with the worst-case scenario in an attack chain. The more significant the impact and the fewer vulnerabilities that must be exploited to achieve that impact, the higher the severity.

Critical	Vulnerability is an otherwise high-severity issue with additional security implications that could lead to exceptional business impact. Examples include trivial exploit difficulty, business-critical data compromised, bypass of multiple security controls, direct violation of communicated security objectives, and large-scale vulnerability exposure.
High	Vulnerability may result in direct exposure including, but not limited to: the loss of application control, execution of malicious code, or compromise of underlying host systems. The issue may also create a breach in the confidentiality or integrity of sensitive business data, customer information, and administrative and user accounts. In some instances, this exposure may extend farther into the infrastructure beyond the data and systems associated with the application. Examples include parameter injection, denial-of-service, and cross-site scripting.
Medium	Vulnerability does not lead directly to the exposure of critical application functionality, sensitive business and customer data, or application credentials. However, it can be executed multiple times or leveraged in conjunction with another issue to cause direct exposure. Examples include brute-forcing and client-side input validation.
Low	Vulnerability may result in limited exposure of application control, sensitive business and customer data, or system information. This type of issue only provides value when combined with one or more issues of a higher risk classification. Examples include overly detailed error messages, the disclosure of system versioning information, and minor reliability issues.
Informational	Finding does not have a direct security impact but represents an opportunity to add an additional layer of security, is considered a best practice, or has the possibility of turning into an issue over time. Finding is a security-relevant observation that has no direct business impact or exploitability, but may lead to exploitable vulnerabilities. Examples include poor communication between engineering organizations, documentation that encourages poor security practices, and lack of security training for developers.