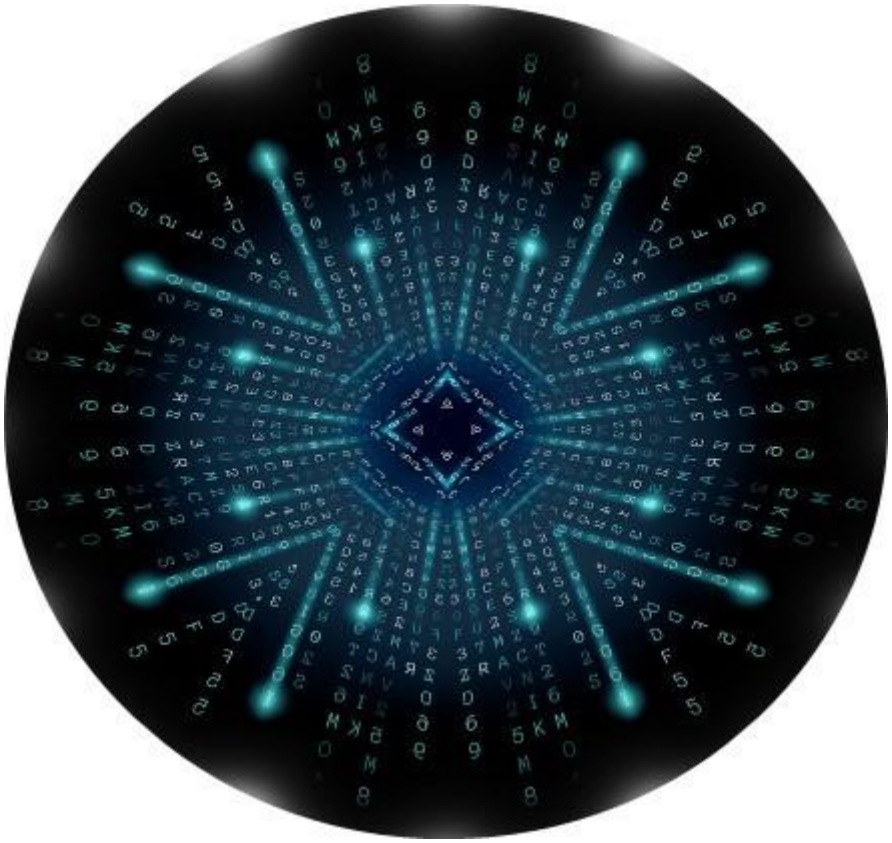
Deloitte.



Adobe Systems India Private Limited

Adobe ColdFusion2021 – Revalidation testing of bug fixes for the findings from Adobe ColdFusion Security Assessment

Report Date: Dec 9, 2020

Disclaimer:

This report has been produced based on the output of the revalidation testing of bug fixes for the High and Medium severity findings from security assessment of Adobe ColdFusion 2021 (CF) and Adobe ColdFusion 2021 Performance Monitoring Toolset (PMT) application that was conducted from 16th November 2020 to 25th November 2020. All vulnerabilities have been highlighted in the report assuming that the utilities and other applications installed on the systems were being used for business purpose, and accordingly, the recommendation to mitigate those vulnerabilities have been made. It is, therefore, recommended that prior to acting on the recommendation, the following actions are taken:

- Ascertain whether a utility or application for which vulnerability has been identified and recommendation is made is actually required in the system for business purposes. In case there is no requirement of such utilities or applications, the same may be removed or disabled following an appropriate process. Else, it is recommended that the recommendations provided are applied to the system

- Relevant backup and rollback plans are made prior to implementing the recommendation on the production system

- Vulnerabilities identified were as based "On the Day" the scan was carried out and also as per the "Scan Policies" (non-intrusive) & "Plugins" selected for the target systems. There may be vulnerabilities, which may not have been assessed since their exploits may lead to system downtime. These vulnerabilities were reported based on the version obtained during the tests. Hence before applying any fixes, confirm these version details of the affected host. Also, the vulnerabilities identified after the scan date may also not form part of this report

- Service packs, hotfixes, patches must be tested on a representative non-production environment prior to being deployed to production to gauge the impact of such changes

- Third-party web site links provided in the recommendation sections of the report are for reference purposes only. Deloitte does not take any responsibility on the web site link and any change in the content

Contents

Introduction

Deloitte Touche Tohmatsu India LLP ("Deloitte") was engaged by Adobe Systems India Private Limited ("Adobe") to perform the revalidation testing of bug fixes for the High and Medium severity findings from security assessment of Adobe ColdFusion 2021 (CF) and Adobe ColdFusion 2021 Performance Monitoring Toolset (PMT) application.

1.1. Objective

The activity was initiated to perform revalidation testing of bug fixes for the High and Medium Severity vulnerabilities shared by Adobe.

The objectives of this assessment were to:

- Perform revalidation testing for the bug fixes and perform confirmatory testing on the High and Medium severity vulnerabilities remediated by Adobe.

1.2. Approach and Methodology

A four-phase approach was adopted to revalidate the bug fixes for the vulnerabilities shared by Adobe team. Each phase is described below.

1.2.1 Phase I – Project Planning and Initialization

The activities of this phase were to:

- Conduct kick-off meetings with Adobe
- Finalize engagement scope and objectives
- Define rules of engagement
- Develop a project plan
- Identify and allocate resources for the project
- Arrange for the necessary technical logistics
- Finalize the deliverable format
- Confirm URL of the application

The binaries were downloaded from the below links:

https://cfdownload.adobe.com/pub/adobe/coldfusion/PR/cf2021gm/ColdFusion_2021_WWEJ_win64.zip
https://cfdownload.adobe.com/pub/adobe/coldfusion/PR/cf2021gm/ColdFusion_2021_PerformanceMonitoringToolset_WWEJ_win64.exe

1.2.2 Phase II –Evaluate

The following activities were performed during phase II:

- Gather information about the bug fixes for the High and Medium severity vulnerabilities from Adobe ColdFusion security assessment
- Perform confirmatory testing on the bug fixes

1.2.3 Phase III – Assess

The following activities were performed during phase III:

- Verify manually the existence of the vulnerability in the applications and APIs
- Determine ease of exploitation
- Attempt controlled compromises
- Collect evidences and document status if bug fixes

1.2.4 Phase IV – Reporting

The deliverables consist of a report describing the status of revalidation testing that was performed. Project Management was performed throughout the course of the engagement.

1.3. Scope

The scope of this security assessment included revalidation testing of bug fixes for the High and Medium severity findings from security assessment of CF and PMT Application as shared by Adobe team.Bug fixes

The following table contains the Application URL, API's and binary details provided for revalidation testing by Adobe team.

#	Assessment Type	End-Point/File Details
1	Application URL	• http://127.0.0.1:8500/ • http://127.0.0.1:9101/
2	API endpoints	• Licensing APIs (7) https://coldfusion-stage.adobe.io//claus/ • PMT APIs (25)

		http://127.0.0.1:9101/pms/
3	Desktop Application (Windows) Version:2021.0.0.323925	• ColdFusion_2021_PerformanceMonitoringToolset_WWEJ_win64.exe • ColdFusion_2021_PerformanceMonitoringToolset_WWEJ_win64.exe

During the security assessment of licensing APIs of CF, Deloitte team used Google cloud instance with google account provided by Adobe team.
Security assessment for Adobe ColdFusion 2021 was carried out only on the "Secure + Production profile" mode selected during installation, as it has same functionalities like the other 2 modes, but with more security controls.

1.4. Out of Scope

After discussion with the Adobe team, following are considered to be out of scope for the current assessment.

1. System implementation, design review, business process testing, systems testing, low level design review
2. Any unreleased vulnerability, which includes vulnerabilities that are not assigned any CVE, CWE, OSVDB or Bug IDs
3. Application functionality review
4. Implementation or operationalization of technical, managerial, procedural or any other control is out of scope of this engagement for Deloitte team.
5. However, Deloitte's team would provide timely recommendations to Adobe Systems India Private Limited in completing these activities within the timelines by providing appropriate templates, sample documents, know-how, guidance, subject matter expertise and will also be involved in review of these documents to make sure appropriateness and conformance to the control objectives identified
6. Network resiliency tests and network security testing

In addition to the above, following functionalities or modules from Adobe ColdFusion are considered to be out of scope from testing.

- Flex Integration
- CORBA connector
- Event Gateway
- Flash Integration
- SOLR server
- PDF Servlet
- Wienre Server

- All Cache engine Servers (EHCache, JCS, Redis, Memcached)
- All the package manager modules (only integration is in scope)

Error and Actuator Licensing APIs that were not available in the application has been discussed with the Adobe team and excluded from the testing.

1.5. Timelines

- The Adobe ColdFusion Application revalidation testing was conducted from 16-November-2020 to 25-November-2020.

Executive Summary

The following sections in the report highlight the status of revalidation testing performed on the High and Medium severity bug fixes from Security Assessment of CF and PMT Application.

Observation status post revalidation:

The revalidation testing was conducted from 16th November 2020 to 25th November 2020 and the below listed High and Medium severity issues were fixed.

Given below table shows the status of observation post revalidation. Only High and Medium severity vulnerabilities were in scope for revalidation testing.

Sl. No	Vulnerability	Severity Rating	Revalidation status as on 25th Nov 2020
1	Application level "DOS" attack is possible in Adobe ColdFusion application	**High**	**Fixed**
2	The application does not terminate existing user sessions upon account deletion	**Medium**	**Fixed**
3	Vulnerable to Stored XSS via System Probe Name Parameter	**Medium**	**Fixed**
4	Stored XSS in Mobile Secret Key	**Medium**	**Fixed**
5	Stored XSS in Mobile Server Context	**Medium**	**Fixed**
6	Stored XSS on Cloud Credentials	**Medium**	**Fixed**
7	Stored XSS in Java Applet	**Medium**	**Fixed**
8	Vulnerable to Stored XSS via CFX Tags in Java CFX Tag Name Parameter	**Medium**	**Fixed**
9	Vulnerable to Stored XSS via CFX Tags in C++ CFX Tag Name Parameter	**Medium**	**Fixed**
10	Stored XSS on Data & server in PDF Service Name Parameter	**Medium**	**Fixed**
11	Stored XSS at Data sources in Driver name under the "other" driver type	**Medium**	**Fixed**

12	Reflected XSS in "No SQL Database" sources HOST parameter	**Medium**	**Fixed**
13	Vulnerable to Stored XSS via Scheduled tasks in "Task name"	**Medium**	**Fixed**
14	Reflected XSS at gateway instances in configuration field parameter	**Medium**	**Fixed**
15	Insecure data storage: System probe passwords are being stored in plain text	**Medium**	**Fixed**
16	Insecure Cache handling in Adobe ColdFusion	**Medium**	**Fixed**

2. Appendix – Severity Rating

The Deloitte Touche Tohmatsu India LLP team used the following criteria to rate the findings in this report.

3.1. Severity Rating

The scale mentioned below was used to rate the severity of the observed vulnerabilities.

Risk Level	Description
Critical	This severity level represents a critical weakness in the current security posture of the product, and requires management's immediate attention to proceed further, considering the security of customer information, impact to the organization and external compliance requirements.
High	This severity level represents a substantial weakness in the current security posture of the product, and requires management's immediate consideration and action to meet minimum baseline.
Medium	This level of vulnerability represents a moderate level of weakness in the current security posture of the product and requires management action attention in the near term.
Low	This severity level provides for an opportunity to improve the current security posture of the product.
Info	This severity level does not have a direct security impact but could help an adversary to gain a better understanding of the product to launch further attacks

Disclaimer

This report has been published based on the output produced by the revalidation testing that was conducted from 16-Nov-2020 to 25-Nov-2020. The vulnerabilities identified were based on the point in time the revalidation testing was carried out and were reported on the basis of the version and instance of the product provided to us during the tests.

- End of Report –

Deloitte.