Adobe Systems Incorporated

Adobe Connect 9.2 Hosted Solution

June 20th 2014

10 Glenlake Pkwy | Suite 130 | Atlanta, GA 30328 | Phone: +1.877.563.4230 | Info@securisea.com
Fax: +1.415.804-4076

Table of Contents

Engagement Overview

On behalf of Adobe Systems Incorporated (Adobe) Securisea performed a grey-box software security assessment of Adobe Connect 9.2 hosted software product during Q2 of 2014. The assessment was intended to evaluate the overall security and robustness of the Adobe Connect 9.2 application as operated in Adobe's Hosted environment. This engagement consisted of many forms of testing including blackbox penetration testing, software reverse engineering and code analysis, XML API fuzzing, static analysis of underlying java bytecode, as well as detailed review of Adobe deployment and configuration documentation. Additionally, Securisea performed a consecutive assessment of the Adobe Connect 9.2 Licensed product, which also included a review of recommended installation procedures for that application. The results in this report are based on Securisea's findings as well as Adobe's subsequent follow-up to those findings.

About Adobe Connect 9.2

Adobe Connect 9.2 is a web conferencing application which brings multiple parties together by providing virtual conference rooms which parties can enter to see online presentations, share documents, and provide other multimedia online content while simultaneously discussing said content over a shared phone conference line. The product works seamlessly for anyone who has common desktop software including a web browser and Adobe Flash® Plugin. Since Adobe Flash® is installed on virtually all existing desktops, Adobe Connect 9.2 effectively requires no additional client software to operate.

The server software runs as a J2EE application under an Apache web stack on Windows Server. Application state is stored in a SQL Server database which can be local or on a remote server. A number of application subcomponents exist to support integration with various VoIP systems, as well as added content management.

About Securisea

Securisea is an independent information security company. Typical engagements include code and architecture reviews, network vulnerability testing, remediation of security exposures, audit support and compliance, security product selection consulting, secure code development, reverse engineering, security policy development and comprehensive training for our clients' internal security staff. Founded in 2006, Securisea is privately held and profitable.

Scope

The scope of this engagement included the full software suite for the Adobe Connect 9.2 Hosted solution including all installed modules. The engagement did cover aspects of how Adobe Connect 9.2 interoperates within a customer environment. However the engagement did assume certain minimal reasonable security precautions would be in place in a typical customer environment which included a reasonable desktop configuration that included regular installation of security patches.

The assessment covered any potential security threat against a typical Adobe Connect 9.2 installation, with an emphasis on common web application issues. The common issues considered included all OWASP Top 10 items, which are:

- Injection Attacks
- Cross-site Scripting (XSS)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross-site Request Forgery (CSRF)
- Security Misconfiguration
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

Assessment Methodology

Securisea consultants used a variety of techniques to determine the security posture of the Adobe Connect 9.2 application. These techniques included but are not limited to:

- **Spidering** – Using automated tools to determine the entire link structure of the application thus enumerating all existing accessible links
- **Manual fault injection** – Securisea consultants created customized application requests to determine if security risks were in fact present
- **Automated fault injection** – Fuzzing tools were used to make a large number of application requests in order to find cases were the application might have a difficult-to-find security risk
- **Web application scanning** – Various web application scanners were run against the application to find common security issues
- **Code analysis** – Securisea examined the logic in the underlying application bytecode to look for cases where security checks might be missing
- **Risk analysis** – Once a potential issue is identified, a number of techniques are employed to determine the actual nature of the risk, if any:

- **Exploit development** – An actual exploit for the issue is developed to determine if it is real or not
- **Impact analysis** – The issue's outcome is examined within the context of the typical Adobe Connect 9.2 operating environment to determine the typical business risk

Policy and Procedure Review

Adobe provided a number of security policy and procedure documents. These documents were reviewed both on and off site. Additionally, relevant Adobe employees were interviewed at its San Francisco office to confirm that various procedures were in place. No formal audit of the procedures was performed.

Secure Development Lifecycle Process

Adobe has a comprehensive secure development lifecycle (SDLC) process. The process documents provided to Securisea showed that Adobe's SDLC process is developed centrally by its Adobe Secure Software Engineering Team (ASSET). Procedures are then implemented in partnership with product engineering and quality engineering teams such as those working on Adobe Connect 9.2. The following processes are in place to various extents in Adobe's SDLC:

- Threat modeling of applications
- Security testing plans
- Secure development training provided by ASSET
- Regular network vulnerability scanning
- External software security reviews

These processes, including the partnership with ASSET in particular provide risk mitigation for security issues that may arise within product code during development.

Personnel Security

Adobe was also found to have good personnel security. This includes both a policy that required background checks on all full time employees, as well as a policy that dictates that access to Adobe Connect 9.2 computing resources be revoked for employees who leave Adobe or transfer to a different department within Adobe.

Software Security Engagement Findings

It was found that Adobe Connect 9.2 had a good suite of security features for protecting customer communications and information. The features could be broadly viewed as falling into one of these following categories:

- **User authentication** – including password management
- **Authorization** – including enforcement of XML API security levels and ACLs, as well as configurable user security levels and permissions
- **Auditing and logging** – including a configurable application logging function

Throughout the applications, numerous security features exist to provide the above objectives. Overall Securisea observed that Adobe Connect 9.2 has sufficient security properties to provide the aforementioned security functions. Additionally, Securisea also tested Adobe Connect 9.2 for robustness against many security vulnerability types. The following details our finding per a sample of types:

Cross Site-Scripting (XSS)

Using a wide array of testing methods including fuzzing, manual testing, embedding script tags into uploaded content and other techniques, Securisea observed that Adobe Connect 9.2 performs a variety of anti-XSS checks. These include checking various inputs for potentially malicious script tags, other aspects of the software perform HTML encoding of all user controllable output. These and other control mechanisms in the software work together to mitigate the risk of XSS within Adobe Connect 9.2.

Injection Flaws

Using a wide array of testing methods, including fuzzing, automated scanning, static code analysis and other techniques, Securisea observed that Adobe Connect 9.2 performs a variety of anti-SQL injection checks. These include performing parameterized SQL queries in every instance Securisea could find except one. In the one case where parameterized queries were not used, whitelist validation of inputs was performed. These and other control mechanisms in the software work together to mitigate the risk of SQL injection and other injection flaws within Adobe Connect 9.2.

Malicious File Execution

Securisea examined the Adobe Connect 9.2 application for malicious file execution by uploading a variety of malicious files. Various techniques were used including malicious extensions, directory traversal attacks, encoded file names, embedded null attacks and other methods. Securisea observed that Adobe Connect 9.2 performs a variety of anti-

malicious file execution checks. These include validating the extensions, names, paths and contents of files to be uploaded. These and other control mechanisms in the software work together to mitigate the risk of malicious file execution flaws within Adobe Connect 9.2.

Insecure Direct Object Reference

Throughout the assessment, Securisea observed that Adobe Connect 9.2 performs a variety of input checks which prevent insecure direct object reference attacks. These include validating many inputs for correctness before processing as well as expanding out full file paths before allowing uploads. These and other control mechanisms in the software work together to mitigate the risk of insecure direct object reference items within Adobe Connect 9.2.

Failure to Restrict URL Access

Using a wide array of testing methods, Securisea observed that Adobe Connect 9.2 performs some level of authorization for all non-public URLs. These tests included attempting to access restricted URLs using a variety of methods and formats, including utilizing multiple server paths for various requests. The preventative checks found included enforcing all user permissions on various forms of non-public content. These and other control mechanisms in the software work together to mitigate the risk of insecure direct object reference items within Adobe Connect 9.2.

In addition to traditional security testing, Securisea validated that Adobe Connect 9.2 has a good breadth of features to enable various compliance controls within the application. Although too numerous to mention individually, some of the key features include:

- Type based content restrictions via content 'pods' which can be enabled and disabled per meeting
- Meeting recordings and detailed logs. Meetings can be recorded for both video and audio. This is important for compliance with various regulations in different jurisdictions
- Controlled access to meetings

Session Management

Using a wide array of testing methods including fuzzing as well as manual and automated scanning, Securisea validated Adobe Connect 9.2's session management features. While Adobe Connect 9.2 is currently vulnerable to CSRF attacks, the other aspects of the application's session management are generally secure. The entropy used in all session

tokens provides sufficient security. Sessions themselves are timed out within appropriate intervals. Additionally, Adobe Connect 9.2 allows for tiered session tokens which differentiate between a login session and a given meeting. These and other control mechanisms in the software work together to provide very solid session management within Adobe Connect 9.2.

Hosted Environment Security

Adobe's Connect 9.2 hosted environment was found to be well secured. The data centers used were industrial strength buildouts including strong doors with locks, video monitoring, physical access logs, secured windows among other controls.

In particular the following stood out in regards to the hosted environment:

- The data centers are in well constructed, physically secured buildings
- The hosted environment is broken into clusters which are operationally identical and thus provide good failover and redundancy
- Existing backup facilities are physically and logically separated from production systems
- The data centers used have good power backup through the use of backup generators and occasionally connections to multiple power grids
- The data centers have good fire suppression capabilities throughout each facility

Securisea has also verified that Adobe maintains good change management and change control practices for its hosted environment which include:

- Document control
- Change management systems
- Backup restoration
- Incident response capability (in partnership with ASSET)
- Compliance Controls