



Adobe Systems Incorporated
Adobe Acrobat Connect Pro
October 28, 2009

1. ENGAGEMENT OVERVIEW

1.1 Overview

At the request of Adobe Systems Incorporated (Adobe), Neohapsis performed a blackbox security assessment of the Adobe Acrobat Connect Pro (Connect Pro) on-premise deployment solution during the period of Q1 2009. The goal of the assessment was to evaluate the overall security posture of the Connect Pro (version 7.0 sp3) application in an on-premise deployed environment. The assessment consisted of both manual and automated attempts to assess the design and implementation of the security mechanisms in use by Connect Pro. In addition, Neohapsis also evaluated the physical and environmental controls as well as provided security policies and procedures that Adobe has employed to protect the production environment. A separate report addresses the assessment of the Connect Pro in a hosted licensed environment.

A supplemental review of version 7.5 (build r122) was performed in October 2009, with a narrow focus on the Compliance and Control feature set. A separate report addresses the assessment of the Connect Pro in a hosted licensed environment.

1.2 About Adobe Acrobat Connect Pro

Connect Pro is web conferencing software that enables instant communication and collaboration through easy-to-use, easy-to-access online personal meeting rooms. Connect Pro enables anyone using a web browser and the Adobe Flash® Player runtime to join a web meeting without having to download cumbersome software. Because the Adobe Flash Player is installed on more than 98 percent of Internet-connected computers worldwide, the experience of joining an online meeting is hassle-free.”

1.3 About Neohapsis

Founded in 1997, Neohapsis helps organizations assess their critical business processes and build a consistent and sustainable risk management discipline to generate lasting value. Our heritage of providing superior IT risk management services and security consulting combined with our award winning Governance, Risk Management, and Compliance (GRC) technology enables organizations to move beyond discrete mitigation and compliance solutions to a comprehensive framework where risk can be transformed into information and opportunity.

1.4 Scope

In Q1 2009, Neohapsis assessed the Connect Pro on-premise solution. Neohapsis consultants assessed both the overall design as well as the implementation of Connect Pro. Assessment of the design focused on validating the existence of a sufficient feature to enforce a desired security policy. Assessment of the security implementation focused on the identification of vulnerabilities that would allow a malicious user to subvert a desired security policy. The vulnerability assessment primarily focused on common application vulnerabilities, including:

- Cross Site Scripting (XSS)
- Broken Authentication and Session Management
- Malicious File Execution
- Insecure Direct Object Reference
- Failure to Restrict URL Access
- Information Leakage and Improper Error Handling
- Injection Flaws
- Insecure Cryptographic Storage
- Insecure Communications

In Q4 2009, Neohapsis performed an assessment of the Compliance and Control feature set. Neohapsis consultants assessed both the overall design as well as the implementation of the compliance module. Assessment of the design focused on validating the existence of a sufficient feature to enforce a desired security policy. Assessment of the security implementation focused on the identification of vulnerabilities that would allow a malicious user to subvert a desired security policy.

Adobe provided policies and procedures were also reviewed for content and compared to industry best practices. Validation of implementation of the policies and procedures was not performed.

1.5 On-premise Solution Assessment Methodology

Neohapsis consultants used both manual and automated attack techniques in an attempt to bypass the intended functionality and secure design of the Connect Pro on-premise application. This included an analysis of the application using 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, etc.) using primarily automated analysis techniques
- Data correlation
 - Research vulnerabilities
 - Eliminate false positives
 - Investigate the extent of the findings

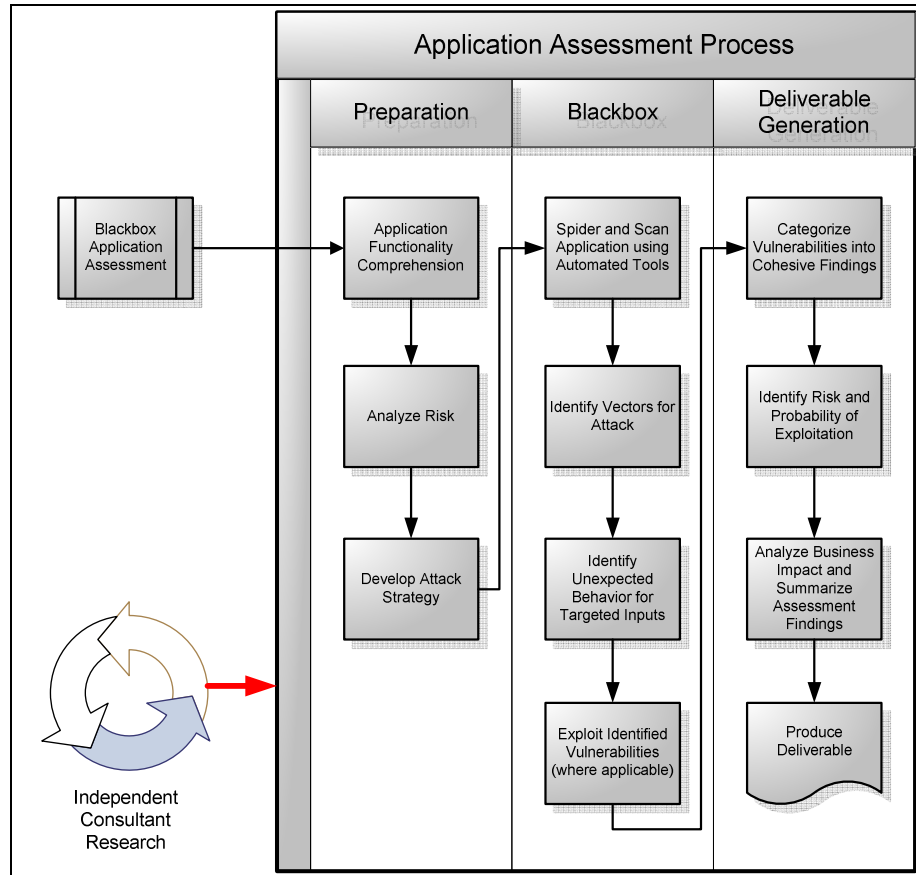


Figure 1 Blackbox Application Assessment Approach

1.6 Policy and Procedure Review

Adobe selected policies and procedures were reviewed for included content and applicability to industry security and operational practices. The material was reviewed remotely at Neohapsis offices and supplemented with phone interviews. No audit of implementation was performed.

1.6...1 Secure Development Lifecycle Policy and Process

Neohapsis reviewed policies, process and supporting evidentiary artifacts associated with Adobe Connect Pro’s secure development lifecycle. Interviews were also conducted with members of the Adobe Secure Software Engineering Team (ASSET), Quality Engineering, and Product Management. Adobe was found to have a formal process which includes:

- Threat modeling at the feature and product architecture level.
- Security design reviews for features.
- A security test plan, based on the threat model.
- Source code reviews.
- A security readiness review conducted as the product nears release.

1.6...2 *Product Security Incident Response*

Neohapsis reviewed policies, and process associated with Adobe Connect Pro's secure development lifecycle. Interviews were also conducted with members of the Adobe ASSET team, Quality Engineering, and Product Management. Adobe was found to have a formal process and an assigned Product Security Incident Response Team (PSIRT) to effectively deal with security vulnerabilities discovered by Adobe or independent third parties. The process includes:

- Formal assignment of resources
- Formal and documented tracking from report to remediation
- Formal internal and external communications
- Testing of remediation
- Independent verification of remediation, if required
- Formal communication of issues and resolution solutions to the Adobe customer base

1.6...3 *Privacy Policy and Protection of Personal Information*

Neohapsis reviewed the Adobe Online Privacy Policy, General Information Security Policy, Adobe Enterprise Security Practices and the Connect Pro Website. In addition, Neohapsis reviewed the TRUSTe website. Finally, Neohapsis discussed the claims and associated materials with Adobe product management. Adobe was found to:

- Provide clear direction and policy regarding the access control to, protection and guardianship of, and a restricted and defined use for, personal information submitted by customers and users of Connect Pro
- Be a current licensee of TRUSTe and is certified by TRUSTe as meeting Safe Harbor requirements.

1.6...4 *Information Security Audits*

Neohapsis has conducted independent third party audits on the Connect Pro release 7.0 and subsequently on the new feature release 7.5 as outlined elsewhere in this document. Additionally, Neohapsis has reviewed the results of consecutive Adobe internal vulnerability scans to validate that Adobe conducts regular scans of the Connect environment for application, OS, and network level vulnerabilities using the Qualys QualysGuard Vulnerability Management solution to maintain a secure hosting environment.

1.6...5 Personnel Security

Neohapsis reviewed the Adobe Online Privacy Policy and the General Information Security Policy. Additionally, Neohapsis discussed the claims and associated materials with Adobe staff. Adobe was found to have:

- A policy requires background checks for all full-time employees, including those who will be administering systems or have access to customer information.
- A policy which requires terminated access for administrators or Connect Pro support personnel leaving adobe or moving to another Adobe department.

2. SOFTWARE SECURITY ENGAGEMENT FINDINGS

Connect Pro employs a variety of measures to secure its customer's communications and data. These security measures address the following categories:

- **User Authentication:** Users must be required to authenticate prior to accessing private content and meetings, and the authentication method itself must occur securely.
- **Password Management:** Users should be required to choose strong passwords and change them regularly.
- **Data Management:** Strong encryption must be used to secure communications and sensitive data stored in the database. Queries to the database must prevent malicious injection.
- **User Privileges:** Access to resources must be configurable and properly allow or restrict access to content and meetings.
- **Auditing and Logging:** For auditing purposes, potentially malicious use must be logged along with date, time and source information.

Each of the above security goals is implemented with a number of security features. Security features include those features whose explicit function is to enforce a security goal. As an example, the login component is a security feature. Neohapsis was able to validate that Connect Pro provides a sufficient set of security features to implement effective control over the above stated goals.

However, security features are only the basis for a secure implementation. Any component within Connect Pro that may affect the security posture of the application is security relevant. For example, Connect Pro allows users to share content by uploading files. File uploading is not a security feature, but is security relevant, as failure to securely handle file uploads may lead to arbitrary code execution on the server. Therefore, beyond validating Connect Pro provides a sufficient set of security features, Neohapsis' primary focus was validating that the security relevant features are implemented in a manner that does not allow a malicious user to subvert the desired security policy of Adobe and their customers.

Using a combination of automated and manual analysis, Neohapsis assessed Connect Pro for common web application vulnerabilities. Section two details Neohapsis' findings for each vulnerability class under evaluation.

2.1 Cross Site Scripting

“XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.”

Using a combination of manual and automated testing, Neohapsis found Connect Pro resilient against XSS attacks. The application validates untrusted user input using a combination of

whitelist and/or blacklist approaches. A whitelist ensures that untrusted user input conforms to an acceptable character set and format. A blacklist leverages a list of potentially malicious input to validate user input. As an example, Connect Pro validates that email addresses conform to a specific format and character set and will not accept any input that does not match. Where a whitelist and/or blacklist is not used, the application encodes untrusted user input when displayed to the user. This prevents the browser from interpreting untrusted user input as valid HTML markup, thus mitigating the possibility of malicious JavaScript injection and execution.

2.2 Injection Flaws

“Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker’s hostile data tricks the interpreter into executing unintended commands or changing data.”

Using a combination of manual and automated testing, Neohapsis found Connect Pro to be resilient against injection-based attacks. Injection attacks can occur in a number of scenarios including SQL queries, LDAP queries, and XPATH queries. Connect Pro makes extensive use of SQL queries throughout the application and Neohapsis did not identify any injection related vulnerabilities during the course of the assessment.

2.3 Malicious File Execution

“Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.”

Using extensive manual testing, Neohapsis found Connect Pro to be resilient against malicious file execution based attacks. Connect Pro mitigates this potential vulnerability using a defense in depth strategy that leverages both a secure design as well as a secure implementation. By design, Connect Pro reduces the threat surface of the application by restricting the number of locations where users can upload files. In those locations where users may upload files, Connect Pro rigorously validates their content type. In addition, Connect Pro restricts uploaded files to a specific directory hierarchy and prevents directory traversal attacks that attempt to break out of this directory.

2.4 Insecure Direct Object Reference

“A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.”

Using a combination of manual and automated testing, Neohapsis found Connect Pro to be resilient against direct object reference attacks. Applications that are vulnerable to direct object reference attacks often fail to leverage secure abstractions that prevent malicious users from interacting directly with low-level system operations. This can manifest itself in a number of ways, such as passing directory names, file names, or SQL queries in user parameters. Neohapsis did not identify any instances where Connect Pro directly references a low-level construct, such as those just listed, in a user parameter. As an example, though Connect Pro allows users to upload content, all file operations occur through an abstraction that prevents direct manipulation of the underlying file system.

2.5 Information Leakage and Improper Error Handling

“Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.”

Using a combination of manual and automated testing, Neohapsis found Connect Pro generally resilient against information leakage attacks. Information leakage attacks can occur in a many number of ways. Some of the more common problems include insecure exception and error handling.

Insecure exception handling occurs when an application fails due to some unforeseen situation and the application returns an error message that, while potentially useful to an application developer, may reveal details about the internal implementation of the application that can be leveraged by a malicious user. Neohapsis found Connect Pro mitigates this attack by returning useful error messages that reveal minimal information to a malicious user. Neohapsis identified a finite number of instances where an exception was thrown and the details were returned to the user. However, this was atypical, and the identified instances did not reveal any sensitive user or critical system information.

In contrast to insecure exception handling, insecure error handling occurs when an anticipated error occurs and the application explicitly discloses more information than necessary to the user. As an example, many applications differentiate between an invalid username and an invalid password during login, providing different error messages for each. However, this may allow an attacker to brute-force valid usernames, which itself may be valuable. Connect Pro securely handles this scenario, and returns the error, “Invalid user or password. Please try again.” Similarly, throughout Connect Pro, Neohapsis did not identify the disclosure of any potentially sensitive information due to insecure error handling.

2.6 Broken Authentication and Session Management

“Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.”

Using a combination of manual and automated testing, Neohapsis found Connect Pro to be resilient against authentication and session management attacks.

In addition to following the secure design and implementation practices detailed in the other findings, an authentication system must also implement a number of secure operational practices. Connect Pro uniquely identifies a user based on a combination of username and password. The user transmits their username and password over a secured SSL/TLS connection, mitigating the possibility of disclosing their credentials during transmission. In addition, Connect Pro allows for the customization and enforcement of various aspects of password management including setting password lifetime duration, enforcing a minimum password length, and enforcing a minimum password complexity.

Once authenticated, secure session management protects an authenticated user from unauthorized users attempting to perform actions on their behalf. Secure session management must provide security for the entire lifetime of the session: from the initial authentication, throughout the duration of the user's session, until the user logs out of the application. Connect Pro uses a combination of best practices to implement each of these phases. First, Connect Pro generates a cryptographically strong session cookie for each user upon visiting the site. This cookie contains approximately seventy-one bits of entropy, minimizing the chance that a malicious user will be

able to predict a user's session cookie. Throughout the user's session, Connect Pro protects the sensitive session cookie by encrypting all communications over SSL/TLS. Finally, upon logout, Connect Pro invalidates the session cookie, both on the client and server, preventing a malicious user from replaying prior requests.

2.7 Insecure Cryptographic Storage

“Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.”

Using a combination of manual and automated testing, Neohapsis was unable to identify any evidence of plaintext storage of sensitive user and system information. Within Connect Pro, the most sensitive information stored by the application is related to user passwords. Connect Pro does not provide any facility to retrieve a forgotten password. Either a user must submit a request to receive an email with a password reset link, or they must contact the system administrator to reset the password on their behalf. Neohapsis was able to validate the use of password hashes, rather than plaintext or reversibly encrypted passwords, within the database. Storing hashed passwords makes the recovery of plaintext passwords more difficult for a malicious user. Using hashed passwords is a good security practice and is an essential component of using secure cryptographic storage for password management.

2.8 Insecure Communications

“Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.”

Using a combination of manual and automated testing, Neohapsis found Connect Pro to be resilient against insecure communication attacks. Insecure communication attacks typically involve a malicious user “sniffing” sensitive user information while the data is in transit from the user's browser to the communicating server. Connect Pro uses SSL/TLS to prevent the disclosure of sensitive information to other users. Moreover, Connect Pro can be configured to require the use of SSL/TLS, and will not accept requests over an unprotected connection. Finally, Connect Pro follows best practices by setting the “Secure” flag on all sensitive session cookies, mitigating the possibility of accidental disclosure over an insecure connection.

2.9 Failure to Restrict URL Access

“Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.”

Using a combination of manual and automated testing, Neohapsis found Connect Pro to be resilient against unauthorized URL access attacks. The Connect Pro groups users into various roles such as Administrators, Authors, and Meeting Hosts. Based on this role, Connect Pro either grants or denies access to various features within the application. Neohapsis conducted numerous tests to attempt submitting requests under a user role that should not have access to the corresponding functionality; all such tests failed. Connect Pro uses a site-wide authorization scheme that validates each request against a role based access control policy. All unsuccessful request submissions either respond with an “unauthorized” message or simply forward the user to the login page.

2.10 Compliance Control Feature Set

Using manual testing, Neohapsis validated Connect Pro's Compliance and Control feature set. Neohapsis found that in addition to security functionality, Connect Pro offers a set of features for compliance and control. These options aim to make the web conferencing experience more compliant with internal auditing policies or governance rules. They give systems administrators a tighter control over the functionality accessible to meeting hosts and meeting participants. Thus, they are useful to mitigate the risk of accidental sharing of sensitive information during live meeting sessions.

Compliance and control settings cover three major areas:

1. Prevents accidental sharing of undesired functionality: Administrators can restrict certain functional modules, named "pods", or sharing features that should not be used in meetings
2. Record and retain communications for auditing purposes: Administrators can lock down the recording settings for all meetings, log chat messages in files and show a notice or disclaimer to participants
3. Control access to meetings: meeting hosts can disable guest access so that guests can no longer request entry. Hosts can also automatically deny access to specific users and groups. Unlike the two previous categories, meeting access control settings are enforced on a per-meeting basis, not for the entire system or hosted account.

3. CONCLUSION

Neohapsis found the design and implementation of Connect Pro resilient to attack under the evaluation criteria detailed in section two. It is the opinion of Neohapsis that Adobe has prioritized security during the software development lifecycle, and as a result, has implemented a product that continually strives to address information security best practices.