



Adobe® Secure Software Engineering

Adobe applies security best practices when building its products so that organizations can deliver more secure, trusted, and engaging user experiences

Executive summary

Adobe uses industry-leading secure software engineering practices and processes in building its products. We create products that are trusted throughout the world to provide engaging experiences while meeting the security needs of organizations and individual users. This document provides an overview of the secure software engineering practices at Adobe.

Experience matters

Adobe has been a leading developer of software for over 20 years. During that time, our products have undergone intense scrutiny from security experts within and outside of Adobe. Our processes have also benefited from years of validation and improvement.

Due to their popularity and usefulness, Adobe products are targets for people who hack, attack, disrupt, and attempt to circumvent the security of software applications. Still, Adobe has maintained a strong, consistent record of providing trusted products, as demonstrated by the continued reliance of many organizations, such as governments and financial institutions, on Adobe software to perform diverse tasks:

- Adobe Flash® Player and Adobe Reader® are the most widely distributed applications in the world.
- Macromedia® ColdFusion® is one of the most widely adopted server platforms for developing dynamic HTML applications.

- Adobe Dreamweaver® and GoLive® are the most widely used tools for building websites worldwide.
- Adobe LiveCycle® interactive process management software is used daily to streamline and automate business processes more securely and effectively.
- Adobe Acrobat® and Creative Suite® software are used extensively by knowledge workers and designers alike for creating, collaborating on, and publishing content.

Our philosophy

When it comes to engineering products for security, Adobe is practical and grounded by its own experience and that of industry peers. We apply industry best practices to product development and quality engineering and to the organization of our processes.

We work hard to provide secure, trusted technology so that our customers can focus on providing rich, user-friendly experiences.

Our internal team

Adobe has a team dedicated solely to making sure that its products are designed, engineered, and validated using security best practices. The Adobe Secure Software Engineering team has industry-leading experience in building secure applications and is a core service provided to all Adobe product teams, independent of any specific business or product line.

Security issues are typically less visible and more complex than other product design elements such as user interface changes or new features. The Secure Software Engineering team of security experts provides visibility into these issues and helps ensure that all security concerns are met before Adobe products go to market.

Development checks and balances

Adobe product teams are dedicated to providing organizations with a product that meets user needs for security. Adobe's engineers consider potential threats when designing and implementing products. Quality engineering (QE) uses those threats to test the products for potential security flaws.

Each product has a dedicated point of contact on the Adobe Secure Software Engineering team who provides ongoing support to engineering and QE. These contacts provide feedback to the product team at well-defined checkpoints in the product lifecycle:

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

Adobe's secure software engineering practices incorporate research and development efforts including automated source code analysis and input validation testing. In addition, the Secure Software Engineering team and product teams regularly hire external security experts to extend and verify the effectiveness of internal work. Adobe also provides secure software engineering training to product engineering and QE teams so that their skills stay sharp.

Incident response process

Occasionally, third-party security vendors, partners, and/or Adobe internal teams may

uncover a potential vulnerability in one of our products that could expose organizations to undesirable security risk. Adobe's Product Security Incident Response Team (PSIRT) provides a number of mechanisms for communicating about potential security issues.

The preferred method for alerting Adobe about potential security vulnerabilities is by contacting the PSIRT directly. The Adobe Security Report Form mailbox at www.adobe.com/misc/securityform.html is monitored by the PSIRT and can be used to provide details about an issue. You can also contact the PSIRT directly to report an incident at PSIRT@adobe.com.

When Adobe becomes aware of a potential security issue, the PSIRT coordinates with representatives from the product engineering team to identify an appropriate remediation, which often includes a patch or a simple workaround.

Releasing information about a potential vulnerability while a fix is still in development could expose consumers to risk. So Adobe tightly controls information about the issue until all potential stakeholders of an appropriate solution are notified.

Once a solution is available, we notify our customers about the potential security vulnerability by posting an Adobe Product Security Bulletin or Adobe Product Security Advisory on the Adobe website at www.adobe.com/support/security.

Adobe also provides a free notification service that distributes information about security advisories and bulletins.

Communication

Adobe is constantly striving to improve communications about security. Through open communication with the user community, we continue to identify and incorporate security best practices into the product development lifecycle, allowing organizations to be confident that Adobe products meet their security needs.

For more information about security and Adobe products, visit www.adobe.com/security.



Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Adobe, the Adobe logo, Acrobat, ColdFusion, Creative Suite, Dreamweaver, Flash, GoLive, LiveCycle, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2007 Adobe Systems Incorporated. All rights reserved. Printed in the USA.
95008935 3/07