

Adobe Secure Product Lifecycle

Building security into Adobe products at every step



Adobe SPLC at a glance

- Industry-leading secure software development best practices, processes, and tools
- Security activities integrated into every stage of the product development lifecycle
- Built on the best practices of industry peers
- Implemented by dedicated product security and incident response teams
- Complemented by ongoing community engagement to constantly improve and evolve

The Adobe Secure Product Lifecycle (SPLC) is a rigorous set of industry-leading best practices, processes, and tools designed to keep customers safe and more secure in the evolving threat landscape as they deploy and use Adobe software. The SPLC touches all aspects of the product lifecycle—from providing essential security training for software development teams and building security features into product design, to developing quick incident response plans postship.

Security concerns are at the top of the agenda for IT professionals and consumers alike. Attacks are becoming increasingly sophisticated, with both targeted and indiscriminate exploits created for profit by patient and highly resourceful entities. The SPLC provides a combination of secure software development best practices, process governance, rigorous testing, and design reviews, and ongoing training for all Adobe product teams to help ensure Adobe software reduces the risk posed by these evolving threats. The SPLC also enables Adobe to respond effectively when issues arise. This effort helps customers remain focused on using Adobe platforms and technologies to create, manage, deliver, and engage with information more powerfully and effectively.

Our philosophy and expertise—Adobe has been a leading developer of software for over 25 years. Adobe products have undergone rigorous testing from security experts within and outside Adobe. Our processes have benefited from years of validation and continuous improvement. The Adobe SPLC process was inspired by other industry-leading secure software development processes, including the Microsoft Security Development Lifecycle (SDL). Adobe has dedicated teams of security experts throughout the organization helping to ensure products are designed, engineered, and validated according to the SPLC.

The Adobe Secure Software Engineering Team (ASSET)—ASSET provides industry-leading experts in building more secure applications to complement our individual product security teams. Security issues are typically less visible and more complex than other product design elements. ASSET provides visibility into these issues and helps ensure that all security concerns are met before Adobe products go to market. Dedicated ASSET engineers provide feedback to the product team at multiple checkpoints in the product lifecycle to help ensure that risk mitigation and user safety requirements are met.

The Adobe Product Security Incident Response Team (PSIRT)—PSIRT is the first line of defense for customers when vulnerabilities in Adobe products are discovered. When Adobe becomes aware of a potential security issue, PSIRT coordinates with representatives from the product engineering team to identify an appropriate plan of response. PSIRT keeps customers updated on each situation with mitigation and update release schedules via the PSIRT blog at blogs.adobe.com/psirt, and Adobe Product Security Bulletins or Adobe Product Security Advisories at www.adobe.com/support/security. Knowledge gained through this process feeds back into further refinement of the SPLC.

Community engagement—Adobe recognizes that working together with our peers and customers is a critical component in effectively mitigating real-world risk. We invest in ongoing programs and activities to engage directly with independent security researchers, commercial security vendors, and customers. We are active members in established industry consortiums such as Software Assurance Forum for Excellence in Code (SAFECode), FIRST, and Open Web Application Security Project (OWASP), and participate in the development of security initiatives such as Building Security in Maturity Model (BSIMM). We also enable our security teams to constantly collaborate with external researchers via conferences, symposiums, and other activities.

Core SPLC elements

- Security training and certification for all product teams
- Product health, risk, and threat landscape analysis
- Full review of the security architecture for each product
- Secure coding guidelines, rules, and analysis
- Review of source code to eliminate known flaws that could lead to vulnerabilities
- Full readiness review, response plans, and release of developer education materials
- Coordinated incident response should vulnerabilities be uncovered postship

The Adobe SPLC process

All product development at Adobe must adhere to the SPLC. The SPLC consists of more than 80 best practices, processes, tools, and metrics for building more secure software.



The Adobe SPLC process

The Adobe SPLC builds security into every step of the product development lifecycle:

Training and certification—Helps to ensure all internal teams are trained and certified on the SPLC process and keeps teams informed of the latest approaches to software security

Planning—Provides an overall health and risk assessment of a product and facilitates any necessary adjustments based on the current threat landscape

Design—Builds defenses against potential threats directly into the initial design of new products and features, and offers an opportunity to improve the security profile of existing features

Implementation—Helps avoid coding issues that could lead to vulnerabilities and leverages state-of-the-art development tools to assist in building more secure code

Testing—Verifies approaches used in building software to mitigate threats and subjects code to rigorous third-party tests that further reduce risk

Ship—Reviews and validates response plans and protocols and educates customers on any new security capabilities available to them as part of the release

Response—Helps to ensure transparency and quick response should issues occur postship, and guides development and release of patches for issues that arise

For more information
www.adobe.com/security



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

Adobe and the Adobe logo 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.

© 2010 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

91027897 06/10