

Adobe Incident Response and Management

Resolving vulnerabilities and mitigating threats quickly, effectively, and thoroughly

Through years of experience, PSIRT has developed a detailed, seven-step process to ensure that Adobe quickly, effectively, and thoroughly responds to and resolves vulnerabilities and threats.



The Adobe Secure Software Engineering Team (ASSET) team proactively focuses on preventing security vulnerabilities in Adobe products before they ship, but Adobe knows that ensuring security doesn't end when a product is released. If external security researchers, partners, or customers discover a vulnerability after a product ships, the Adobe Product Security Incident Response Team (PSIRT) responds to resolve the security issue quickly, effectively, and thoroughly. PSIRT is your first line of defense for vulnerability resolution and threat mitigation. PSIRT coordinates with Adobe product engineering teams to identify the appropriate response plan and keeps you informed on mitigation procedures and release schedules.

Supplementing the internal Adobe incident response and management process is our partnership in the Microsoft Active Protections Program (MAPP). MAPP facilitates advance information sharing of product vulnerabilities with security software providers, such as antivirus and intrusion detection and prevention vendors, allowing them to reduce the risk of malicious coders exploiting the vulnerability.



Adobe incident response and management process

Through years of experience, PSIRT has developed a detailed, seven-step process to ensure that Adobe quickly, effectively, and thoroughly responds to and resolves vulnerabilities and threats.

Step 1: Receive, log, and report

PSIRT receives information about security vulnerabilities from numerous channels, including:

- Email from security researchers, partners, and customers
- Public posting at Bugtraq, SecurityFocus, and so on.
- Adobe Support
- Internal notification, typically from Adobe engineering teams, quality engineering teams, or ASSET

When the report is received, PSIRT responds to the individual to get more information and possibly a proof-of-concept file to demonstrate the vulnerability.

To track the issue, PSIRT logs it in the Adobe Incident Response Database. An incident ID is automatically generated, which is passed along to the reporting individual.

Step 2: Analyze and verify authenticity

PSIRT sends the report to the relevant product team's Product Security Response Team (PSRT) for verification. This team includes development, quality, and product engineers and managers. Working together, PSIRT and the product security teams attempt to reproduce the bug and determine its severity. If the bug is reproducible, PSIRT logs an internal Adobe bug for the issue.

Step 3: Investigate and develop mitigation guidance

The Adobe product team investigates the issue and develops a fix or workaround. PSIRT works with the product team to verify the fix. The fix is then ported to all supported versions of the product, as well as any version currently under development.

Step 4: Confirm issue and deliver preliminary bulletin

PSIRT responds back to the individual who reported the problem that it has been reproduced and a fix is being developed. As soon as possible, PSIRT sends a timeline for the patch to the individual.

Adobe encourages the coordinated disclosure of vulnerabilities in our products, so we request that the reporting individual or researcher keep the vulnerability confidential until Adobe makes a fix available. Our goal is to keep our customers as secure as possible, so we place a high priority on keeping vulnerability information out of the hands of malicious hackers.

Step 5: Develop and verify patch

The Adobe product team produces a patch to resolve the issue for all supported product versions as quickly as possible. During this step, PSIRT communicates all relevant status updates to the reporting individual and answers any questions that arise.

PSIRT then produces an Adobe Security Bulletin draft regarding the issue. Before publication, all internal Adobe stakeholders review the bulletin.

Step 6: Issue final public security bulletin

When possible, PSIRT provides the patch and the Adobe Security Bulletin to the reporting individual for verification and review. Included in the bulletin is an acknowledgement to the reporting individual in uncovering and resolving this issue. In addition, PSIRT works with the MITRE Corporation to generate Common Vulnerabilities and Exposures (CVE) identifiers for any relevant issues. CVE identifiers help partners and IT administrators track fixes for potential issues.

Step 7: Distribute patch through certified channels

PSIRT posts the Adobe Security Bulletin to www.adobe.com/support/security along with the patch and posts a link to the bulletin on the PSIRT blog at <http://blogs.adobe.com/psirt> to inform customers who subscribe to the RSS feed for discovered threats and vulnerabilities. In addition, PSIRT coordinates a notification email to customers who have signed up for this service. Customers can use the patch to update their product installations to mitigate the vulnerability.

Report issues to Adobe PSIRT

To report a potential security threat or vulnerability, use the feedback web form at www.adobe.com/misc/securityform.html or email PSIRT@adobe.com.

Stay up to date on security issues

To subscribe to the Adobe PSIRT RSS feed, visit <http://blogs.adobe.com/psirt/feed>.

To receive PSIRT security notification emails, visit www.adobe.com/cfusion/entitlement/index.cfm?e=salert.

For more information
www.adobe.com/security



Adobe

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. Mac OS is a trademark of Apple Inc., registered in the U.S. and other countries. Intel is a trademark of Intel Corporation in the U.S. and other countries. All other trademarks are the property of their respective owners.

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

12/10