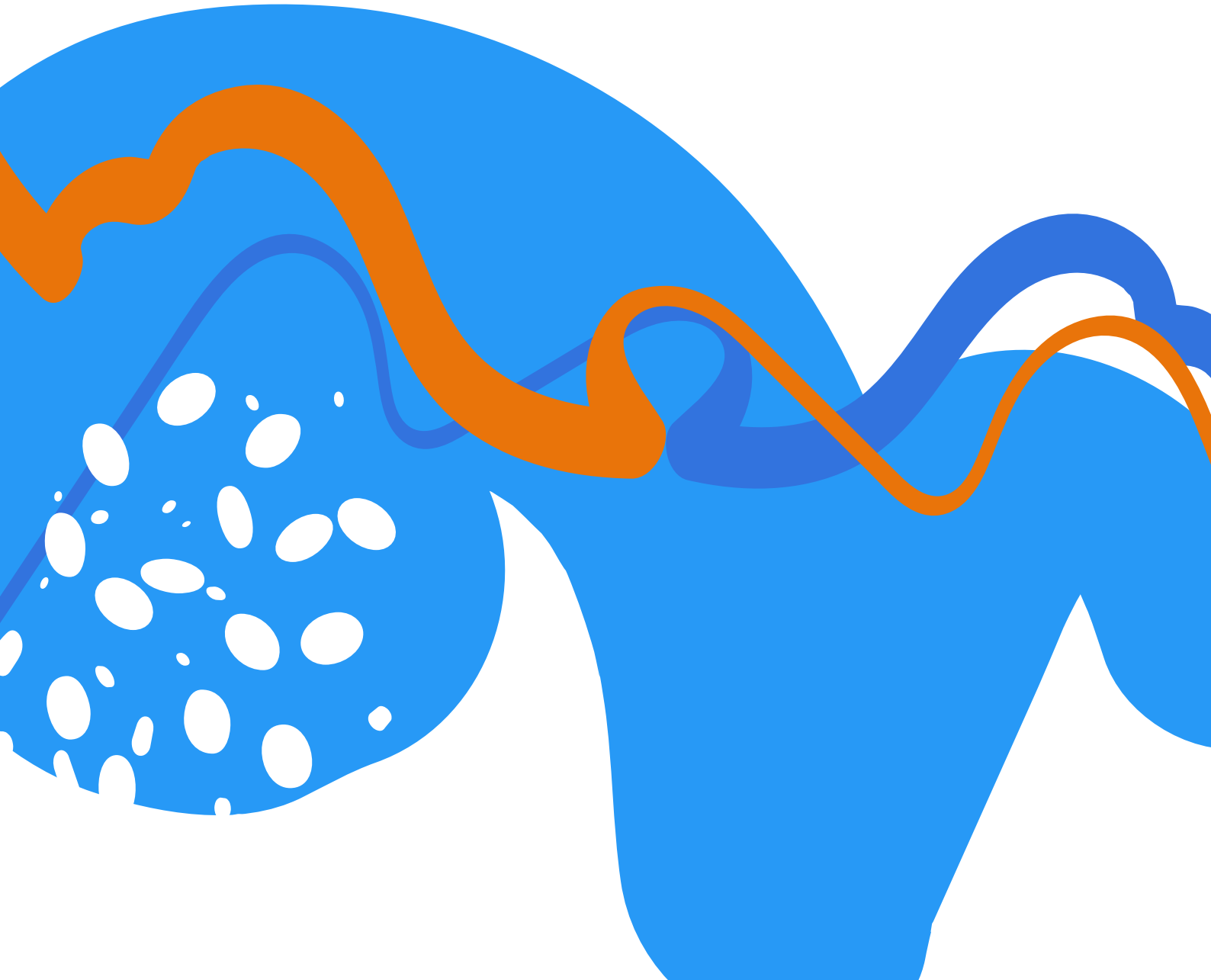
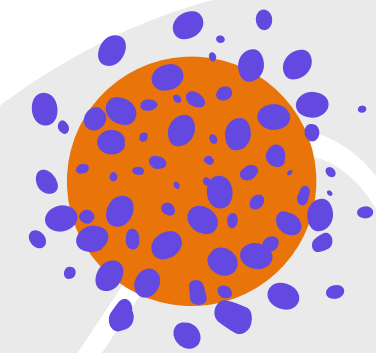
DOCUMENTO TÉCNICO

Información general sobre la seguridad de las aplicaciones de Adobe



Índice de contenidos



Introducción

En Adobe®, el desarrollo de aplicaciones seguras es esencial para lo que hacemos; por ello, hemos realizado importantes inversiones en investigación y tecnología en materia de seguridad. Nuestro equipo encargado de la seguridad de las aplicaciones, que se centra en mantenerse al día del ritmo de la innovación al tiempo que ayuda a garantizar que los productos y servicios de Adobe incluyan las medidas de seguridad más eficaces, trabaja con los equipos de productos y servicios de toda la empresa para diseñar aplicaciones que incorporen una seguridad de serie. El equipo también se basa en distintos enfoques de automatización para recopilar datos y ayudar a tomar decisiones basadas en los riesgos que mejoren la posición de seguridad general de la empresa.

En este documento técnico, se describe la estrategia de seguridad de las aplicaciones de Adobe, que se centra en introducir controles de seguridad desde el principio del ciclo de desarrollo para ayudar a crecer, reducir los costes generales y minimizar las posibilidades de que aparezcan riesgos reales de seguridad; todo ello refuerza nuestro compromiso con las prácticas de seguridad modernas que protegen los datos y los flujos de trabajo de Adobe y de nuestros clientes.

Estrategia de seguridad de las aplicaciones de Adobe

La estrategia de seguridad de las aplicaciones de Adobe se centra en solucionar de raíz los problemas de seguridad, en lugar de tratar los síntomas. Para ello, aplicamos la resolución en origen e introducimos la seguridad desde el principio del ciclo de desarrollo de las aplicaciones. Al establecer controles y mecanismos de seguridad en las fases de requisitos, arquitectura, diseño y programación del desarrollo, ayudamos a afianzar los controles de seguridad y a reducir el elevado coste de los cambios que se introducen durante las fases de prueba posteriores. Este enfoque también minimiza las posibilidades de que aparezcan riesgos reales de seguridad, lo que se traduce en una mayor seguridad para nuestros clientes.

Ciclo de vida seguro de los productos de Adobe

El ciclo de vida seguro de los productos (SPLC) de Adobe, que está integrado en el ciclo de vida de los productos de software —desde el diseño y desarrollo hasta la garantía de calidad, prueba e implementación—, es la base de todos los esfuerzos de seguridad de Adobe. El SPLC, un riguroso conjunto de varios cientos de actividades específicas de seguridad, define procesos y capacidades claros y repetibles para ayudar a los equipos de desarrollo a incorporar la seguridad en nuestros productos y servicios.

El SPLC de Adobe está implementado en toda la empresa, y los investigadores de seguridad del equipo de seguridad de las aplicaciones de Adobe, que asesora a nuestros equipos de productos y servicios sobre las prácticas recomendadas para los controles de seguridad y valida estos controles mediante la automatización, se encargan de verificarlo. Los controles del SPLC de Adobe incluyen planificaciones, herramientas de seguridad y métodos de pruebas que guían al equipo de seguridad a la hora de hacer frente a los 10 defectos más graves de seguridad de aplicaciones de Open Web Application Security Projects (OWASP) y a los 25 errores principales de software de CWE/SANS. Puedes encontrar más información sobre el SPLC de Adobe en el centro de confianza de Adobe.

Pila de seguridad de las aplicaciones de Adobe

En Adobe, el diseño de aplicaciones seguras parte de la pila de seguridad de las aplicaciones. Los equipos de productos empiezan utilizando plataformas que incorporan la seguridad de serie, verifican sus aplicaciones con diversas capacidades de seguridad automatizadas y lo entrelazan todo con revisiones de seguridad y pruebas manuales.

Las tres capas de la pila incluyen un conjunto de herramientas y servicios basados en las prácticas de seguridad modernas, centradas en proteger los datos y los flujos de trabajo de los clientes, que los equipos de productos de Adobe pueden utilizar en su proceso de desarrollo para garantizar la integración de la seguridad en todas las aplicaciones de Adobe.

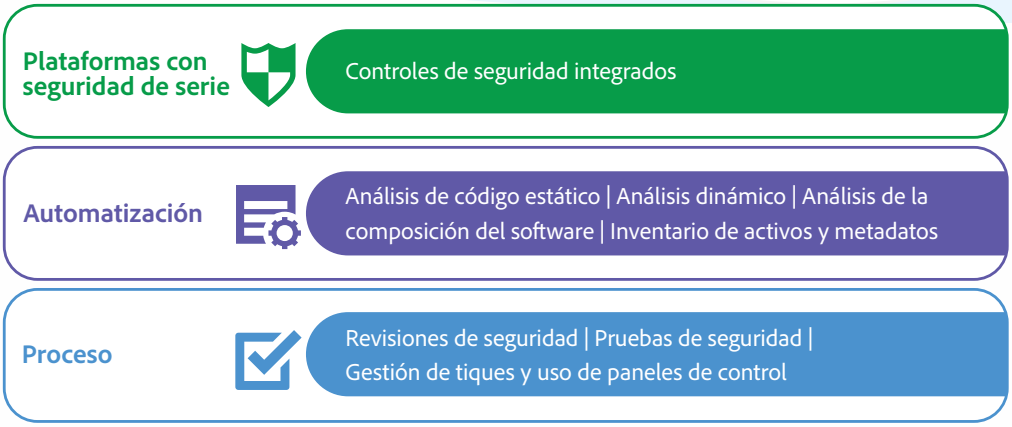


Figura 2: Pila de seguridad de las aplicaciones de Adobe

Plataformas con seguridad de serie

Los desarrolladores de Adobe utilizan plataformas preaprobadas que incorporan la seguridad de serie para crear procesos bien estructurados que proporcionen guías para el desarrollo rápido y seguro de los productos y servicios de Adobe. Estas guías incluyen servicios de identidad y autorización verificados y aprobados, pasarelas de API, sistemas de mensajería, SDK y marcos de trabajo.

Las plataformas con seguridad de serie no solo facilitan la escalabilidad, sino que también ayudan a comprobar la correcta implementación de las funciones y configuraciones de seguridad. Estas plataformas, que se basan en dos principios clave —detección y prevención—, incluyen un conjunto de soluciones de detección continua para identificar posibles usos poco seguros, así como controles preventivos que ayudan a los desarrolladores de Adobe a lograr que sus productos y servicios incorporen la seguridad de serie.

Las plataformas con seguridad de serie ayudan a garantizar lo siguiente:

- **Uso seguro**: al analizar de manera continua un amplio conjunto de datos de configuración, registros y código fuente, podemos identificar rápidamente los errores de configuración de seguridad en nuestros productos y servicios, detectar cualquier desviación y avisar a los equipos de productos correspondientes.
- **Controles de seguridad integrados**: nuestras inversiones en controles de seguridad que siguen las prácticas recomendadas, como los privilegios mínimos, la denegación predeterminada y la autenticación incorporada, ayudan a nuestros equipos de productos a centrarse en su experiencia en los productos, al tiempo que protegen los datos y los flujos de trabajo de los clientes.

Automatización de la seguridad

En Adobe, la automatización permite ampliar la seguridad de las aplicaciones en toda la empresa y proporcionar una cobertura de seguridad continua, a la vez que se mantiene el rápido ritmo de la innovación. Nuestras iniciativas de análisis estáticos y dinámicos, que se centran en el código de software, las recopilaciones de datos de configuración, el tráfico de solicitud/respuesta y los registros de aplicaciones, ayudan a Adobe a hacer que todo el ciclo de desarrollo de software sea seguro.

- **Análisis de código estático**: nuestra plataforma de análisis de código automatizado aprovecha tanto las herramientas de código abierto como las comerciales para analizar los repositorios de código. Transmitimos los comentarios directamente a nuestros desarrolladores en línea con sus flujos de trabajo de desarrollo, cuando los problemas resultan más fáciles de mitigar. Estas herramientas, junto con las capacidades únicas de nuestro entorno, ayudan a Adobe a ofrecer la mayor seguridad posible en nuestro código fuente.
- **Análisis dinámico**: de manera similar a nuestro enfoque con respecto a los análisis de código estáticos, Adobe utiliza herramientas personalizadas y comerciales para identificar las vulnerabilidades de seguridad durante el tiempo de ejecución.
- **Análisis de la composición del software**: supervisamos de manera minuciosa el uso de componentes de terceros en nuestros productos y servicios, y revisamos con regularidad la posición de seguridad de dichos componentes mediante el uso de soluciones internas y comerciales. Cuando encontramos un componente vulnerable o cuya vida útil está llegando a su fin, avisamos a nuestros desarrolladores, lo que ayuda a garantizar su mitigación en el momento oportuno.
- **Inventario de activos y metadatos**: un sofisticado conjunto de metadatos de toda la empresa ayuda a nuestro equipo de seguridad de las aplicaciones a obtener información más detallada sobre los productos y servicios de Adobe.

Proceso

La experiencia y los procesos de seguridad internos de Adobe constituyen la base de nuestras iniciativas de seguridad. Invertimos continuamente en formar en materia de tecnologías y enfoques emergentes tanto a los miembros de nuestro equipo de seguridad como a nuestros expertos en seguridad. La gestión de tiques de asistencia técnica, el uso de paneles de control y la mitigación eficiente de los riesgos a través de la información sobre los adversarios y la creación de modelos de las amenazas crean el tejido que canaliza de manera eficaz las iniciativas de seguridad.

Revisiones de seguridad

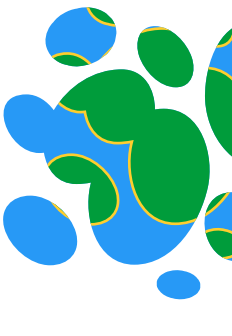
Para proporcionar una garantía de seguridad en todos los productos y servicios de Adobe, emprendemos un proceso de colaboración para identificar los problemas relacionados con la seguridad, determinar el nivel de riesgo asociado a dichos problemas y tomar decisiones fundamentadas sobre la mitigación o aceptación de los riesgos, incluido lo siguiente:

- **Creación de modelos de las amenazas**: realizar un modelo de las amenazas durante la fase de diseño ayuda a identificar los defectos de seguridad al principio del ciclo de desarrollo y crea una sólida base de seguridad para los productos y servicios de Adobe. Creamos modelos de las amenazas para señalar las áreas en las que es posible que se requieran cambios de arquitectura para evitar las amenazas conocidas. El uso de la automatización en el proceso de creación de modelos de las amenazas nos ayuda a adaptarnos a cualquier escala de manera eficaz mediante la generación automática de los requisitos de seguridad, lo que hace que el proceso de revisión sea más eficiente.
- **Revisiones de código específicas**: en el caso de algunas secciones concretas de código que procesen datos confidenciales o de componentes reutilizados por varios servicios, nuestros investigadores de seguridad realizan revisiones de código manuales para asegurarse de que el código cumpla las prácticas recomendadas de seguridad.
- **Pruebas enfocadas**: los investigadores de seguridad de Adobe realizan pruebas de seguridad periódicas de nuestros productos y servicios basándose en varios factores, como el interés de los adversarios y los patrones de ataque conocidos.

Pruebas de seguridad

Además de las revisiones de seguridad periódicas, Adobe realiza pruebas de penetración de nuestros productos y servicios que ayudan a reforzar los puntos débiles identificados e involucra a nuestra comunidad de usuarios con nuestro programa de recompensas por la detección de errores para detectar y notificar los problemas. Entre nuestras actividades de pruebas de seguridad, figuran las siguientes:

- **Pruebas de penetración internas**: los equipos de seguridad interna de Adobe realizan pruebas de penetración asistidas por código mediante el uso de una combinación de técnicas automatizadas y manuales dirigidas a los puntos débiles señalados durante las revisiones de seguridad.
- **Pruebas de penetración externas**: colaboramos con empresas líderes de seguridad de terceros para realizar pruebas de penetración con el objetivo de descubrir posibles vulnerabilidades de seguridad y mejorar la seguridad general de los productos y servicios de Adobe. Tras la recepción de un informe del tercero, Adobe documenta las vulnerabilidades observadas, evalúa la gravedad y las prioridades, y crea una estrategia de mitigación o un plan de corrección. Una vez solucionado el problema, volvemos a realizar las pruebas de penetración para garantizar su resolución.
- **Recompensas por la detección de errores**: Adobe tiene programas internos y externos de recompensas por la detección de errores que recompensan a las personas que descubren y notifican errores de software con un reconocimiento público o una compensación económica. Nuestras recompensas internas por la detección de errores aprovechan el talento de seguridad de la empresa y ayudan a promover la concienciación sobre la seguridad de las aplicaciones en nuestros equipos de ingeniería. Además, Adobe recurre a la comunidad de investigadores de seguridad externos para revelar de forma responsable las oportunidades aprovechables que afectan a Adobe o a nuestros clientes. La revelación responsable de problemas específicos de los productos se incentiva mediante la concesión de compensaciones económicas por las aportaciones válidas.



Gestión de tiques y uso de paneles de control

La gestión automatizada de tiques permite notificar a los equipos de productos las vulnerabilidades de seguridad aprovechadas o aprovechables de las que se tenga conocimiento; de esta manera, pueden mitigar el problema lo antes posible. Los tiques se asignan automáticamente a los equipos en función de sus habilidades, experiencia y conocimiento de los productos. Mediante el uso de paneles de control e indicadores clave de rendimiento (KPI), nuestro equipo de seguridad de las aplicaciones puede medir el grado de adopción de la pila de seguridad de las aplicaciones de Adobe en toda la empresa, así como determinar la eficacia de nuestras soluciones de automatización de la seguridad.

Conclusión

La pila de seguridad de las aplicaciones de Adobe ayuda a los equipos de productos y servicios de Adobe a diseñar aplicaciones que incorporen la seguridad de serie. Al introducir controles de seguridad desde el principio del ciclo de desarrollo, nuestro equipo de seguridad de las aplicaciones ayuda a Adobe a prevenir de forma proactiva los riesgos de seguridad y a mantener la seguridad integral de los productos y servicios de Adobe. Para asegurar este resultado, aprovechamos la automatización y la supervisión continua de nuestra posición de seguridad a través de informes, paneles de control y revisiones trimestrales del cumplimiento normativo.

Adobe

10/22