Ofrecer una base segura para el desarrollo de software

Ante el aumento exponencial de los usuarios maliciosos en Internet y los ciberataques promovidos por gobiernos, creemos que nuestros productos y servicios deben ser tan seguros como útiles. En Google, nos esforzamos más que nunca para proteger a las personas, las organizaciones y los gobiernos compartiendo nuestro conocimiento especializado, capacitando a la sociedad para hacer frente a unos ciberriesgos en constante evolución y trabajando constantemente para impulsar avances en ciberseguridad que permitan construir un mundo más seguro para todos.

El software de código abierto (es decir, aquel que está disponible gratuitamente para que cualquiera pueda utilizarlo, modificarlo y desarrollarlo) es la base del Internet moderno. El ecosistema de desarrollo de software de código abierto permite la colaboración y la aceleración de la innovación mediante el intercambio libre de soluciones. Sin embargo, esa apertura que hace que el mundo digital sea accesible para todos lo hace también especialmente vulnerable a las amenazas de seguridad.

El desafío

La seguridad del software de código abierto preocupa a todos

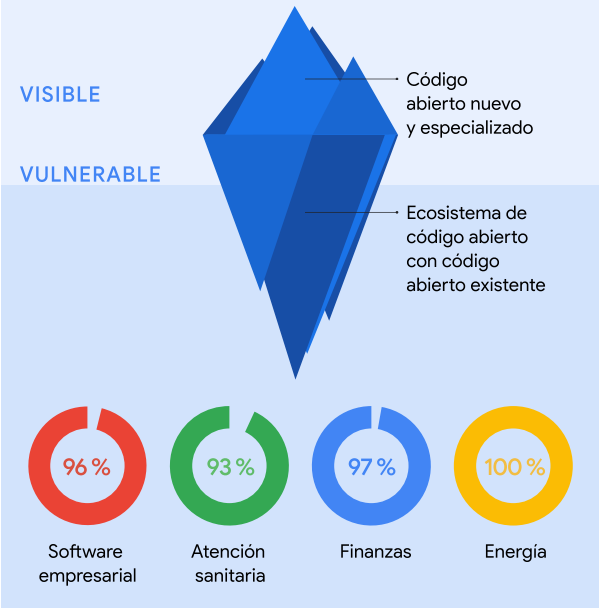
La comunidad del software de código abierto, cuyos pilares básicos son la transparencia y el intercambio, aporta gran parte del código con el que se desarrollan la mayoría de aplicaciones que utilizamos en la actualidad. Las personas confían diariamente en aplicaciones que utilizan código abierto, como los equipos médicos o la red eléctrica, lo que convierte a estos proyectos en un objetivo prioritario para los ciberataques. Durante los últimos tres años, se ha producido un incremento interanual del 742 %[1] en los ataques a la cadena de suministro del software.

El ecosistema del código abierto es una intrincada superposición de capas con dependencias indirectas ocultas que pueden contener fallos de seguridad. Estas capas hacen que las vulnerabilidades resulten difíciles de detectar manualmente. Por ello, proteger esta parte del proceso de desarrollo de software se ha convertido en una necesidad urgente a nivel mundial.

Es necesario reforzar todos los procesos:

- Los desarrolladores de software de código abierto necesitan conocimientos y recursos para proteger sus proyectos
- Las organizaciones deben conocer los riesgos y las vulnerabilidades de la cadena de suministro para elaborar planes de mitigación
- Los gobiernos y el sector deben colaborar en la creación de normas de seguridad sólidas y eficaces[3]

PORCENTAJE DE SOFTWARE INDUSTRIAL QUE CONTIENE CÓDIGO ABIERTO[2]



[2] Fuente: 2022 Synopsys Open Source Security and Risk Analysis Report

Nuestra solución

Proteger el software de código abierto que usamos todos

En Google, llevamos años trabajando para superar este desafío. De hecho, más del 10 % de los empleados de Google colaboran anualmente en proyectos de software de código abierto. Nuestra experiencia nos ha llevado a la conclusión de que apostar por un modelo abierto es la clave para lograr la seguridad digital. Los enfoques abiertos que aplicamos nos permiten adoptar rápidamente las últimas innovaciones y conseguir que más personas puedan resolver sus problemas de seguridad. Pero, para materializar todo el valor que el código abierto puede ofrecer, necesitamos asociaciones público-privadas más sólidas y marcos normativos dinámicos que refuercen la seguridad de todos. Por este motivo, valoramos los esfuerzos del Gobierno de EE. UU. para promover la seguridad del software de código abierto, como la Ley de Seguridad del Software de Código Abierto (Securing Open Source Software Act) aprobada por el Senado en 2022.

- Google está asumiendo un papel de liderazgo dentro de la comunidad con la creación de marcos de seguridad de nueva generación —como SLSA (Supply-chain Levels for Software Artifacts)[4,5] — y el desarrollo de herramientas de seguridad avanzadas.
- Hemos desarrollado GUAC (Graph for Understanding Artifact Composition), una base de datos centralizada y consultable que recopila información sobre seguridad del software procedente de distintas fuentes. GUAC ofrecerá a todas las organizaciones acceso gratuito y práctico a la información sobre seguridad del software, con el objetivo de democratizar la disponibilidad de la misma.

Nuestros compromisos:

- Invertir 100 millones de dólares en seguridad del software de código abierto, roles de liderazgo dentro de la Open Source Security Foundation y colaboraciones directas con desarrolladores
- Definir y compartir las normas prácticas de seguridad, las guías, las herramientas gratuitas y las prácticas recomendadas que utilizamos internamente con toda la comunidad del software de código abierto
- Mejorar la detección, los filtros automatizados y la integración de la seguridad en las primeras fases del proceso de desarrollo
- Automatizar herramientas para ofrecer niveles empresariales de seguridad gratuitos y accesibles para todos

Aplicaciones

Google OSS Fuzz

Nuestra respuesta a la vulnerabilidad Heartbleed

El fallo de seguridad Heartbleed fue una vulnerabilidad grave del código abierto con potencial para afectar a casi todos los usuarios de Internet. Aprovechándola, un grupo de piratas informáticos robó en 2014 los nombres, las direcciones, las fechas de nacimiento, los números de teléfono y los números de la seguridad social de alrededor de 4,5 millones de pacientes de la base de datos de uno de los mayores hospitales de EE. UU.

En respuesta al ataque, Google lanzó el servicio comunitario gratuito OSS-Fuzz. A diferencia de las pruebas manuales, que pueden llevar meses, el fuzzing detecta debilidades de seguridad desconocidas en el software en minutos. Lo que hicimos fue invertir en la creación de una infraestructura para probar automáticamente cientos de proyectos de código abierto. En la actualidad, OSS-Fuzz analiza periódicamente diferentes proyectos de código abierto e innova permanentemente para detectar nuevas clases de errores.

Más de 800 proyectos de código abierto críticos se someten a pruebas de fuzzing en seis idiomas.

Nuestros logros e inversiones en el sector

2020 — AGOSTO
Ingresamos en la Open Source Security Foundation (OpenSSF) con el objetivo de asesorar y mejorar la seguridad del software de código abierto.

2021 — MAYO Y JUNIO
Creamos unas prácticas recomendadas para software de código abierto en cumplimiento del **Decreto Ejecutivo 14028 del Gobierno de EE. UU.** y proporcionamos asesoramiento sobre normas de seguridad para la cadena de suministro del software.

JUNIO
Compartimos el SLSA en la OpenSSF, haciendo público el marco de seguridad interno de Google y permitiendo a todos crear software más seguro.

AGOSTO
Nos comprometimos a invertir 100 millones de dólares en mejorar y proteger el software de código abierto, mediante diversas iniciativas, como una colaboración con desarrolladores para detectar y corregir vulnerabilidades.

2022 — MAYO
Anunciamos la creación del Grupo de Mantenimiento del Código Abierto de Google durante una cumbre en Washington DC, al que asignamos un equipo de desarrolladores a tiempo completo que trabaja directamente en mejorar la seguridad de proyectos de código abierto.

MAYO
Presentamos el producto Assured Open Source Software, que ayuda a integrar en los flujos de trabajo de los desarrolladores los mismos paquetes de código abierto de confianza que utilizamos en Google.

Prácticas recomendadas por Google que pueden ayudar a las organizaciones públicas y privadas a protegerse en el entorno actual:

- Implementar SLSA para reforzar la seguridad de la cadena de suministro del software
- Firmar criptográficamente y verificar la autenticidad del software mediante Sigstore
- Automatizar la detección, el seguimiento y la clasificación de vulnerabilidades con OSS-Fuzz y OSV.dev
- Usar tarjetas de resultados para evaluar automáticamente el riesgo de seguridad en las dependencias

Nuestro enfoque

El eslabón más débil de un software es el que define la seguridad del conjunto. Por ello, Google está invirtiendo sus conocimientos y recursos financieros para mejorar la seguridad de todo el ecosistema del código abierto. Según nuestro equipo de expertos en desarrollo y seguridad, las siguientes actividades nos permitirán proteger a más organizaciones públicas y privadas:

Nuestro equipo audita cada etapa del ciclo de vida del producto realizando continuamente análisis y pruebas de fuzzing para detectar vulnerabilidades.

Defendemos un Internet abierto, compartiendo nuestros conocimientos con la comunidad de desarrolladores y protegiendo a los usuarios individuales y las empresas.

Al detectar amenazas sofisticadas, proporcionar herramientas automatizadas avanzadas y anticiparnos a las tendencias, estamos adaptando la seguridad al futuro.

Proteger el software de código abierto es una responsabilidad compartida y nos comprometemos a seguir colaborando para resolver este problema urgente y crítico. g.co/security/gosst

Referencias: 1. 2022 State of the Software Supply Chain. 2. 2022 Synopsys Open Source Security and Risk Analysis Report. 3. CISA Goes on Tour to Get Feedback on Cyber Incident Reporting Rules. 4. Compartir nuestros conocimientos (como hicimos al publicar el marco SLSA o asesorar a la OpenSSF) permite que todos los que crean software, y no solo Google, puedan beneficiarse de nuestra experiencia y nuestras prácticas de seguridad de eficacia demostrada. 5. SLSA es un conjunto de prácticas que pueden ayudar a las organizaciones a mejorar la seguridad de sus procesos de desarrollo de software. Su aplicación ayuda a cumplir el Marco de Desarrollo Seguro de Software (Secure Software Development Framework), es decir, los requisitos establecidos por el Gobierno de EE. UU. en respuesta al Decreto Ejecutivo sobre ciberseguridad. Gracias a él, las organizaciones dispondrán de una guía para cumplir las directrices federales que especifican cómo hacer que el software sea más seguro para todos.