Protegiendo los cimientos del desarrollo de software

Considerando el incremento radical de los ciberataques patrocinados por gobiernos y actores maliciosos en línea, creemos que nuestros productos y servicios son tan útiles como seguros. En Google, estamos más enfocados que nunca en proteger a las personas, las organizaciones y los gobiernos con nuestra experiencia: capacitamos a la sociedad para combatir los riesgos cibernéticos en constante evolución y trabajamos continuamente para progresar en el arte de la ciberseguridad para construir un mundo más seguro para todas las personas.

El software de código abierto, es decir, el código que se pone a disposición de quien quiera utilizarlo, modificarlo y desarrollarlo, es la base del internet moderno. Al compartir soluciones de manera libre, el mundo del desarrollo de software de código abierto facilita colaborar e innovar de manera rápida. Sin embargo, la misma apertura que hace que el mundo digital sea accesible para todos, también lo hace especialmente vulnerable a las amenazas a la seguridad.

El reto

El software de código abierto es importante para todos

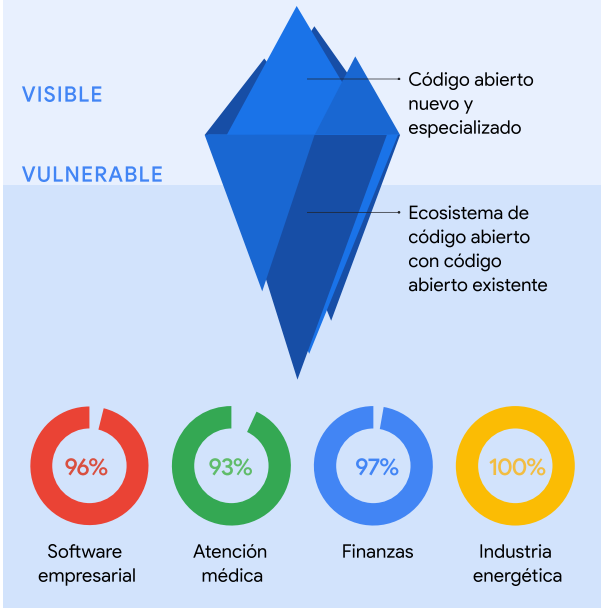
La comunidad de desarrollo de código abierto, basada en la transparencia y el intercambio, aporta una enorme cantidad de código a la mayoría de las aplicaciones que utilizamos hoy en día. Desde equipos médicos hasta la red eléctrica, las personas dependen del software de código abierto (OSS) prácticamente todo el día, lo que convierte a los proyectos de código abierto en un objetivo prioritario para los ciberataques. En los últimos tres años se ha producido un aumento interanual del 742%[1] en los ataques a la cadena de suministro de software.

El ecosistema de código abierto está intrincado en capas, donde las dependencias indirectas ocultas pueden contener fallos de seguridad. Estas capas hacen que las vulnerabilidades sean difíciles de detectar manualmente, y proteger esta parte del desarrollo de software se ha convertido en un problema de seguridad urgente en todo el mundo.

Es necesario prestar más atención en todos los niveles:

- Los desarrolladores de código abierto necesitan conocimientos y recursos para proteger sus proyectos.
- Las organizaciones necesitan comprender los riesgos y vulnerabilidades de la cadena de suministro para desarrollar planes de mitigación.
- Los gobiernos y la industria deben asociarse para garantizar normas de seguridad sólidas y eficaces.[3]

PORCENTAJE DE SOFTWARE EN LA INDUSTRIA QUE CONTIENE CÓDIGO ABIERTO[2]



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

Nuestra solución

Asegurar un Software de código abierto para todos

En Google llevamos años trabajando en este reto. De hecho, cada año más del 10% de los Googlers contribuyen a proyectos de software de código abierto. Nuestra experiencia nos lleva a concluir que la seguridad digital moderna puede ir de la mano de la apertura. Los enfoques abiertos garantizan que podamos adoptar rápidamente las últimas innovaciones y permiten que más personas resuelvan los problemas de seguridad. Pero para aprovechar plenamente el valor del código abierto, necesitamos asociaciones público-privadas más sólidas y marcos políticos dinámicos que refuercen la seguridad para todos. Por eso acogemos con satisfacción 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 presentada en el Senado en 2022.

- Guiamos a la comunidad con marcos de seguridad del mejor nivel, como los niveles de la cadena de suministro para artefactos de software (SLSA),[4,5] y al desarrollar herramientas de seguridad avanzadas.
- Desarrollamos Graph for Understanding Artifact Composition (GUAC), que reúne información de seguridad del software procedente de distintas fuentes en una sola base de datos consultable. GUAC democratizará la disponibilidad de información de seguridad haciéndola libremente accesible y útil para todas las organizaciones.

Nuestro compromiso:

- Invertir 100 millones (USD) en seguridad de código abierto, desempeñar funciones de liderazgo en la Open Source Security Foundation y colaborar directamente con los desarrolladores.
- Definir y compartir con toda la comunidad de código abierto las normas de seguridad aplicables, orientaciones, herramientas gratuitas y prácticas recomendadas que utilizamos internamente.
- Detección avanzada, clasificación automatizada y formas de incorporar la seguridad en las primeras fases de desarrollo.
- Automatizar las herramientas para que la seguridad a nivel empresarial sea gratuita y accesible para todos/as.

Aplicaciones

Google OSS Fuzz

Nuestra respuesta al error Heartbleed

El error Heartbleed fue una grave vulnerabilidad de código abierto: una debilidad con el potencial de afectar a casi todos los usuarios de internet. En 2014, unos piratas informáticos robaron nombres, direcciones, fechas de nacimiento, números de teléfono y números de seguridad social de ~4.5 M de pacientes de la base de datos de uno de los hospitales más grandes en Estados Unidos.

En respuesta, Google lanzó OSS-Fuzz como un servicio comunitario gratuito. El fuzzing localiza puntos débiles de seguridad desconocidos en cuestión de minutos, a diferencia de las pruebas manuales, que pueden llevar meses. Invertimos en la creación de infraestructura para probar automáticamente cientos de proyectos de código abierto. OSS-Fuzz ejecuta ahora escaneos regulares de código e innova constantemente para encontrar otro tipo de errores.

Más de 800 proyectos críticos de código abierto son escaneados mediante fuzzing en seis idiomas.

Nuestras inversiones y logros en la industria

2020 — AGOSTO
Nos unimos a la Open Source Security Foundation (OpenSSF) para guiar y mejorar la seguridad del software de código abierto.

2021 — MAYO Y JUNIO
Establecimos prácticas recomendadas de OSS en cumplimiento con **la Orden Ejecutiva 14028 de la Casa Blanca** y brindamos información sobre las normas de seguridad de la cadena de suministro de software.

2021 — JUNIO
Lanzamos SLSA con OpenSSF para compartir el marco de seguridad interno de Google y permitir a todo el mundo crear software más seguro.

2021 — AGOSTO
Destinamos 100 millones (USD) a mejorar y proteger el OSS, incluida la colaboración con desarrolladores para encontrar y corregir vulnerabilidades.

2022 — MAYO
Presentamos el Equipo de mantenimiento de código abierto de Google durante una **Cumbre en D.C.**: dedicamos un equipo de desarrolladores a tiempo completo a trabajar directamente con proyectos de código abierto para mejorar su seguridad.

2022 — MAYO
Anunciamos el producto Assured Open Source Software, que ayuda a incorporar los mismos paquetes de código abierto de confianza que utiliza Google en los flujos de trabajo de los desarrolladores.

Prácticas recomendadas por Google que pueden ayudar a las organizaciones públicas y privadas a mantenerse seguras hoy en día:

- Implementar SLSA para reforzar la seguridad de la cadena de suministro de software.
- Firmar criptográficamente y verificar la autenticidad de su software con Sigstore.
- Automatizar el descubrimiento, el seguimiento y la clasificación de vulnerabilidades con OSS-Fuzz y OSV.dev.
- Utilizar Tarjetas de resultados para evaluar automáticamente los riesgos de seguridad de sus dependencias.

Nuestro enfoque

El software es tan seguro como su eslabón más débil. Empleamos nuestra experiencia y recursos financieros para aumentar la seguridad de todo el ecosistema de código abierto. Nuestro equipo de expertos en desarrollo y seguridad cree que podemos proteger a más organizaciones públicas y privadas de las siguientes maneras:

Nuestro equipo audita cada etapa del ciclo de vida del producto a través del escaneo, análisis y fuzzing continuos en busca de vulnerabilidades.

Apoyamos el internet abierto, compartimos lo que sabemos con la comunidad de desarrolladores y mantenemos la seguridad del público y las empresas.

Detectamos amenazas complejas y proporcionamos herramientas automatizadas avanzadas. Siempre nos mantenemos un paso delante de lo que venga para preparar a la seguridad para el futuro.

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

Fuentes: 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 (es decir, publicar SLSA, liderar OpenSSF) significa que todos los que crean software, no solo Google, pueden beneficiarse de la experiencia de Google y de sus prácticas de seguridad probadas a lo largo del tiempo, 5. SLSA es un conjunto de prácticas que pueden ayudar a las organizaciones a mejorar la seguridad de su proceso de desarrollo de software. Ayuda al gobierno de EE.UU. a cumplir el Marco de desarrollo de software seguro (requisitos establecidos por el gobierno en respuesta a la Orden Ejecutiva sobre ciberseguridad). Esto significa que las organizaciones dispondrán de orientación sobre cómo cumplir los lineamientos federales para que el software sea más seguro para todos.