Protegendo a base do desenvolvimento de software

Com o aumento de ataques cibernéticos patrocinados por Estados e agentes online mal-intencionados, acreditamos que nossos produtos e serviços só podem ser úteis se forem seguros. No Google, estamos mais focados do que nunca em proteger pessoas, organizações e governos compartilhando nossa experiência; capacitar a sociedade para lidar com o dinamismo dos riscos cibernéticos; e criar mecanismos de segurança cibernética cada vez mais sofisticados e um mundo mais seguro para todos.

O software de código aberto – disponibilizado gratuitamente para qualquer pessoa usar, modificar e desenvolver – é a base da internet moderna. O desenvolvimento de software de código aberto permite colaboração e inovação rápidas e o compartilhamento livre de soluções. Mas a abertura que torna o mundo digital acessível a todos também o deixa vulnerável a ameaças de segurança.

Desafio

O software de código aberto é uma preocupação de todos

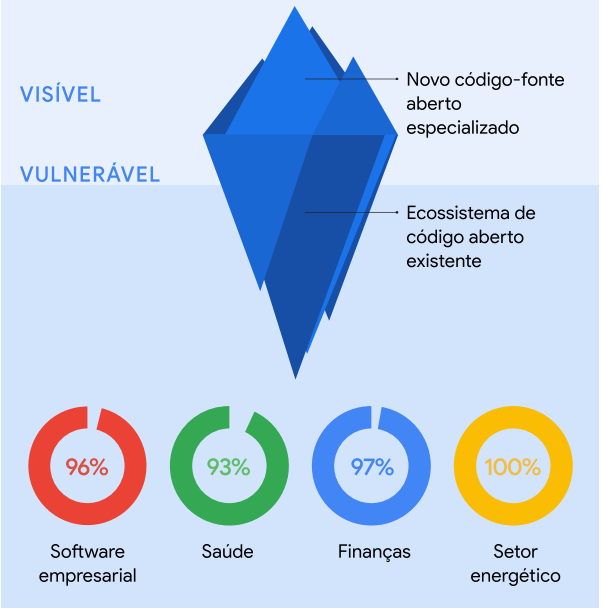
A comunidade de desenvolvimento de código aberto, com base em transparência e compartilhamento, contribui com códigos para a maioria dos aplicativos que usamos hoje. De equipamentos médicos à rede elétrica, as pessoas contam com software de código aberto (OSS) para praticamente tudo, tornando estes projetos um grande alvo de ataques cibernéticos. Nos últimos três anos, houve um aumento de 742%[1] em ataques à cadeia de produção de software.

O ecossistema de código aberto possui camadas intrincadas, e suas dependências indiretas e ocultas podem esconder falhas de segurança. Essas camadas dificultam a detecção manual de vulnerabilidades; por isso, proteger essa etapa do desenvolvimento de software tornou-se uma questão de segurança urgente no mundo todo.

Mais foco é necessário em todos os níveis:

- Os desenvolvedores de código aberto precisam de conhecimento e recursos para proteger seus projetos
- As organizações precisam entender os riscos e as vulnerabilidades da cadeia de produção para traçar planos de mitigação
- Os governos e o setor devem trabalhar juntos para garantir padrões de segurança sólidos e eficazes[3]

PORCENTAGEM DE SOFTWARE DE CÓDIGO ABERTO[2]



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

Nossa solução

Garantindo o software de código aberto para todos

No Google, trabalhamos nesse desafio há anos. A cada ano, mais de 10% dos Googlers colaboram em projetos de software de código aberto. Essa experiência nos leva a concluir que podemos alcançar a segurança digital abraçando a abertura. Com abordagem aberta, podemos adotar rapidamente as últimas inovações para que mais pessoas solucionem desafios de segurança. Mas, para aproveitar ao máximo as vantagens do código aberto, precisamos de parcerias público-privadas mais fortes e estruturas políticas dinâmicas para reforçar a segurança de todos. Por isso, celebramos o trabalho do governo dos EUA para aprimorar a segurança do OSS, como a Lei de Proteção de Software de Código Aberto apresentada no Senado em 2022.

- Estamos liderando a comunidade com estruturas de segurança avançadas, como níveis de cadeia de produção de artefatos de software (SLSA),[4,5] e desenvolvendo ferramentas de segurança avançadas.
- Desenvolvemos o Graph for Understanding Artifact Composition (GUAC), que reúne informações de segurança de software de várias fontes em um único banco de dados consultável. O GUAC vai democratizar as informações de segurança, tornando-as livremente acessíveis para todas as organizações.

Nossos compromissos:

- Investir US$ 100 milhões em segurança de código aberto, funções de liderança na Open Source Security Foundation e colaboração direta com desenvolvedores
- Definir e compartilhar nossos padrões de segurança acionáveis, orientações, e ferramentas e práticas recomendadas gratuitas internos com toda a comunidade de código aberto
- Realizar detecção avançada, triagem automatizada e formas de aumentar a segurança nos estágios iniciais de desenvolvimento
- Automatizar ferramentas para tornar a segurança empresarial gratuita e acessível para todos

Aplicações

Google OSS Fuzz
Nossa resposta ao bug Heartbleed

O Heartbleed bug era uma vulnerabilidade grave de código aberto, com potencial para afetar quase todos os usuários da Internet. Em 2014, hackers roubaram nomes, endereços, datas de nascimento, números de telefone e de previdência de ~4,5 milhões de pacientes do banco de dados de um dos maiores hospitais dos Estados Unidos

Em resposta, o Google lançou o OSS-Fuzz como um serviço comunitário gratuito. O teste fuzz identifica em minutos pontos fracos de segurança desconhecidos, diferente do teste manual, que pode levar meses. Investimos em uma infraestrutura para testar automaticamente centenas de projetos de código aberto. Agora, o OSS-Fuzz executa verificações de código regularmente, sempre inovando para detectar outros tipos de bugs.

Mais de 800 projetos críticos de código aberto são verificados pelo teste fuzz em seis idiomas.

Investimentos e marcos

2020 — AGOSTO
Ingressou na Open Source Security Foundation (OpenSSF) para orientar e melhorar a segurança do software de código aberto

2021 — MAIO E JUNHO
Estabeleceu as melhores práticas de OSS em conformidade com a **Ordem Executiva 14028 da Casa Branca** e contribuiu com orientações sobre padrões de segurança na cadeia de produção de software.

JUNHO
Lançou o SLSA com OpenSSF, divulgando a estrutura de segurança interna do Google para que todos criem softwares mais seguros.

AGOSTO
Prometeu US$ 100 milhões para aprimorar e proteger o OSS,incluindo parcerias com desenvolvedores para detectar e corrigir vulnerabilidades

2022 — MAIO
Anunciou a equipe de manutenção de código aberto do Google durante um **DC Summit,** dedicando uma equipe de desenvolvedores em tempo integral para melhorar a segurança de projetos de código.

MAIO
Lançou o Assured Open Source Software, que ajuda a incorporar os pacotes seguros de código aberto que o Google usa nos fluxos de trabalho de desenvolvimento.

Práticas recomendadas pelo Google para ajudar organizações públicas e privadas a se manterem seguras:

- Implementar o SLSA para fortalecer a segurança da cadeia de produção de software
- Assinar criptograficamente e verificar a autenticidade do seu software usando o Sigstore
- Automatizar a descoberta, o rastreamento e a triagem de vulnerabilidades com OSS-Fuzz e OSV.dev
- Usar Scorecards para avaliar automaticamente o risco de segurança com suas dependências

Nossa abordagem

A segurança do software termina onde começam suas fraquezas Estamos investindo experiência e recursos financeiros para aumentar a proteção de todo o ecossistema de código aberto. Segundo nossa equipe de especialistas em desenvolvimento e segurança, podemos proteger mais organizações públicas e privadas das seguintes maneiras:

Nossa equipe audita todas as etapas do ciclo de vida do produto, verificando, analisando e testando continuamente as vulnerabilidades

Apoiamos a internet aberta, compartilhando o que sabemos com a comunidade de desenvolvedores e mantendo-a segura para o público e as empresas

Estamos preparando a segurança para o futuro, detectando ameaças sofisticadas, fornecendo ferramentas automatizadas avançadas e nos mantendo à frente do que está por vir

Proteger o software de código aberto é uma responsabilidade compartilhada. Estamos comprometidos a colaborar continuamente neste problema crítico e urgente. g.co/security/gosst

Fontes: 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. Compartilhar nosso conhecimento (ou seja, liberar o SLSA, orientar o OpenSSF) significa que todos que produzem software, não só o Google, podem se beneficiar da nossa experiência e práticas de segurança comprovadas pelo tempo. 5. O SLSA é um conjunto de práticas que podem ajudar as organizações a melhorar a segurança durante o desenvolvimento de software. Ele ajuda a atender à estrutura de desenvolvimento de software seguro do governo dos EUA, um conjunto de requisitos estabelecidos pelo governo em resposta à Ordem Executiva de segurança cibernética. Dessa forma, as organizações terão orientações para cumprir as diretrizes federais e tornar o software mais seguro para todos.