



Sécuriser les bases du développement logiciel

Face à la montée en flèche des cyberattaques soutenues par certains États et autres acteurs malveillants en ligne, nous pensons que la sûreté de nos produits et services devient tout aussi importante que leur utilité. Chez Google, nous sommes plus que jamais mobilisés pour **protéger** les personnes, les entreprises et les gouvernements en partageant notre expertise, en **donnant à la société les moyens** de faire face aux cyberrisques en constante évolution et nous efforçant de faire **progresser** les pratiques de pointe en matière de cybersécurité afin de construire **un monde plus sûr pour tous**.

Les logiciels libres, dont le code est mis à la disposition de tous gratuitement pour qu'ils soient utilisés, modifiés et développés, sont la base de l'Internet moderne. En encourageant la collaboration et l'innovation rapide, le monde du développement du logiciel libre contribue au partage gratuit de solutions. Or, la nature même de ces logiciels, qui met le monde numérique à la disposition de tous le rend également particulièrement vulnérable aux menaces de sécurité.

Le défi

Les logiciels ouverts, une affaire qui concerne tout le monde

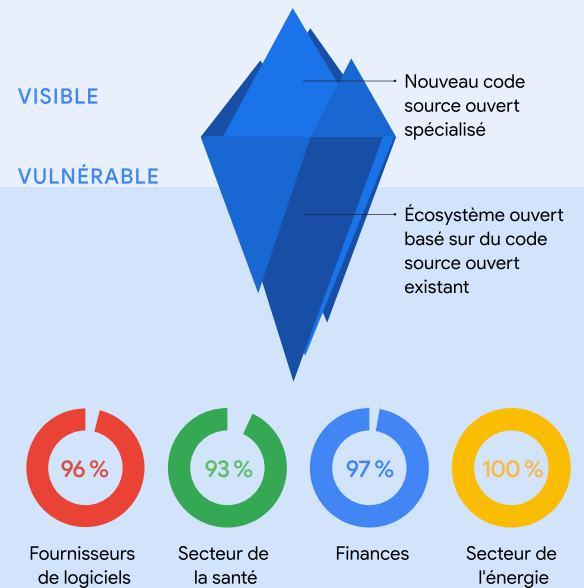
La communauté des développeurs de logiciels ouverts, fondée sur la transparence et le partage, contribue à l'énorme quantité de code qui fait fonctionner les applis que nous utilisons aujourd'hui. Nombre de nos activités (des équipements médicaux jusqu'aux réseaux électriques), dépendent des logiciels ouverts à presque tous les moments de la journée, ce qui fait des projets au code source ouvert une cible de choix des cyberattaques. Au cours des trois dernières années, on note une augmentation de **742 % d'une année sur l'autre**¹ des attaques contre la chaîne d'approvisionnement logicielle.

L'écosystème des logiciels ouverts est composé de couches complexes, indirectement dépendantes, qui peuvent donner lieu à des failles de sécurité. Ces couches rendant les vulnérabilités difficiles à détecter manuellement, la sécurisation de cette partie du développement logiciel est devenue une urgence de sécurité au niveau mondial.

Un attention supplémentaire doit être portée à tous les niveaux :

- ✓ Les développeurs de logiciels ouverts ont besoin d'informations techniques et de ressources pour sécuriser leurs projets
- ✓ Les entreprises doivent prendre conscience des risques et des vulnérabilités de la chaîne d'approvisionnement afin d'élaborer des plans d'atténuation
- ✓ Les gouvernements et les entreprises du secteur doivent s'associer pour garantir des normes de sécurité robustes et efficaces³

POURCENTAGE DE L'INDUSTRIE DU LOGICIEL QUI UTILISE DU CODE SOURCE OUVERT²



² Source : 2022 Synopsys Open Source Security and Risk Analysis Report

Notre solution

Rendre les logiciels ouverts plus sûrs pour tous

Chez Google, nous nous efforçons de relever ce défi depuis des années. En effet, chaque année, plus de **10 % des employés de Google** contribuent à des projets de logiciels ouverts. Notre expérience nous a appris que la sécurité numérique moderne passe par **l'adoption d'une approche basée sur l'ouverture**. Les approches basées sur une sécurité ouverte facilitent la prise en compte rapide des dernières innovations et permettent à un plus grand nombre de personnes de résoudre des problèmes de sécurité. Mais pour exploiter au maximum les apports des logiciels ouverts, nous devons nouer des partenariats public-privé plus solides et avoir des politiques dynamiques pour renforcer la sécurité de tous. C'est pourquoi nous saluons les efforts déployés par le gouvernement américain pour faire progresser la sécurité des logiciels libres, illustrés notamment par la *Securing Open Source Software Act* présentée au Sénat en 2022.

- Nous montrons la voie à la communauté en mettant en place des cadres de sécurité de niveau supérieur, tels que le Supply-chain Levels for Software Artifacts (SLSA),^{4,5} et en développant des outils de sécurité à la pointe de la technologie.
- Avec le Graph for Understanding Artifact Composition (GUAC), nous avons mis au point un outil qui rassemble dans une seule base de données des informations sur la sécurité des logiciels provenant de différentes sources. Le GUAC **mettra à la disposition du plus grand nombre** les informations relatives à la sécurité en les rendant librement accessibles à toutes les entreprises.

Nos engagements :

- ✓ **Investir 100 millions de dollars dans la sécurité des logiciels ouverts**, conforter notre rôle dans les instances dirigeantes de l'Open Source Security Foundation et collaborer directement avec les développeurs
- ✓ **Définir et partager** des normes de sécurité exploitables, des conseils, ainsi que **certains de nos outils sans frais et bonnes pratiques** avec l'ensemble de la communauté des logiciels ouverts
- ✓ **Faire progresser les processus de détection**, le tri automatisé et la manière d'intégrer la sécurité dans les premières phases de développement
- ✓ **Automatiser les outils** pour rendre accessible à tous un niveau professionnel de sécurité



Applications

Programme OSS Fuzz de Google

Notre réponse au Le bogue Heartbleed

Le bogue Heartbleed est le nom donné à une vulnérabilité d'un code source ouvert qui a conduit à une faille grave qui aurait pu toucher la quasi-majorité des utilisateurs d'Internet. En 2014, des pirates informatiques ont volé les noms, adresses, dates de naissance, numéros de téléphone et numéros de sécurité sociale d'environ **4,5 millions de patients** faisant partie de la base de données de l'un des plus grands hôpitaux des États-Unis

En réaction, Google a lancé **OSS-Fuzz, un service sans frais mis à la disposition de la communauté**. Des tests à données aléatoires permettent d'identifier des failles de sécurité inconnues en quelques minutes, contrairement aux tests manuels qui peuvent prendre des mois. Nous avons investi dans la mise en place d'une infrastructure permettant de tester automatiquement des centaines de projets au code source ouvert. OSS-Fuzz effectue désormais des analyses régulières du code et innove constamment pour trouver de nouveaux types de failles.

Plus de 800 projets au code source ouvert critiques sont analysés par Fuzz dans six langues.

Nos investissements dans le secteur et étapes clés



Les pratiques recommandées aujourd'hui par Google pour assurer la sécurité numérique des organismes publics et privés :

- ✓ Mettre en œuvre le cadre SLISA pour renforcer la sécurité de la chaîne d'approvisionnement logicielle
- ✓ Automatiser la découverte de vulnérabilités, le suivi et le tri des vulnérabilités avec OSS-Fuzz et OSV.dev
- ✓ Signer et vérifier l'authenticité de vos logiciels à l'aide de Sigstore
- ✓ Utiliser Scorecards pour évaluer automatiquement les risques de sécurité en fonction de vos dépendances

Notre approche

La sécurité d'un logiciel dépend de son point le plus faible. Nous mettrons notre expertise et nos ressources financières au service du renforcement de la sécurité de l'intégralité de l'écosystème du logiciel ouvert. Notre équipe d'experts en développement et en sécurité est convaincue que nous pouvons protéger un nombre plus important d'organismes publics et privés de la manière suivante :

Notre équipe vérifie chaque étape du cycle de vie du produit, en l'analysant et en testant aléatoirement ses éventuelles vulnérabilités

Nous partageons nos connaissances avec la communauté des développeurs pour un Internet ouvert et sûr, au service du public et des entreprises

Nous assurons l'avenir de la sécurité en détectant des menaces sophistiquées, en partageant des outils automatisés évolués et en gardant une longueur d'avance sur les évolutions sociétales et technologiques



La sécurisation des logiciels ouverts est une responsabilité partagée, et nous sommes déterminés à poursuivre la collaboration sur cette question urgente et grave. g.co/security/gosst

Sources : 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. Partager nos connaissances (diffusion du cadre SLISA et participation à l'OpenSSF, par exemple), c'est mettre notre expérience et nos pratiques éprouvées en matière de sécurité au service de tous ceux qui développent des logiciels, et pas seulement de Google, 5. Le cadre SLISA est un ensemble de pratiques destinées à aider les entreprises à améliorer la sécurité de leur processus de développement des logiciels. Il permet de respecter les exigences du SSDF (Secure Software Development Framework) énoncées par le gouvernement américain en réponse au décret exécutif sur la cybersécurité. Cela signifie que les entreprises peuvent compter sur un ensemble d'orientations sur la manière de se conformer aux directives fédérales afin de rendre les logiciels plus sûrs pour tous.