Securizarea bazei pentru dezvoltarea software

Dată fiind creșterea puternică a atacurilor cibernetice sponsorizate de anumite state și a actorilor rău-intenționați online, credem că produsele și serviciile noastre sunt utile doar în măsura în care sunt securizate. La Google, suntem mai concentrați ca niciodată să protejăm oamenii, organizațiile și autoritățile guvernamentale prin împărtășirea experienței noastre, să ajutăm societatea să facă față riscurilor cibernetice din ce în ce mai mari și să lucrăm permanent pentru a dezvolta o securitate cibernetică de vârf, în vederea construirii unei lumi mai sigure pentru toți oamenii.

Software-ul open source — codul care este pus la dispoziție gratuit pentru oricine dorește să-l utilizeze, să-l modifice și să construiască pe baza lui — este baza internetului modern. Lumea dezvoltării software-ului open source permite colaborarea și inovația rapidă, prin permiterea accesului la soluții în mod gratuit. Dar însăși deschiderea care face lumea digitală accesibilă tuturor o lasă deosebit de vulnerabilă în fața amenințărilor de securitate.

Provocarea

Software-ul open source este o preocupare pentru toată lumea

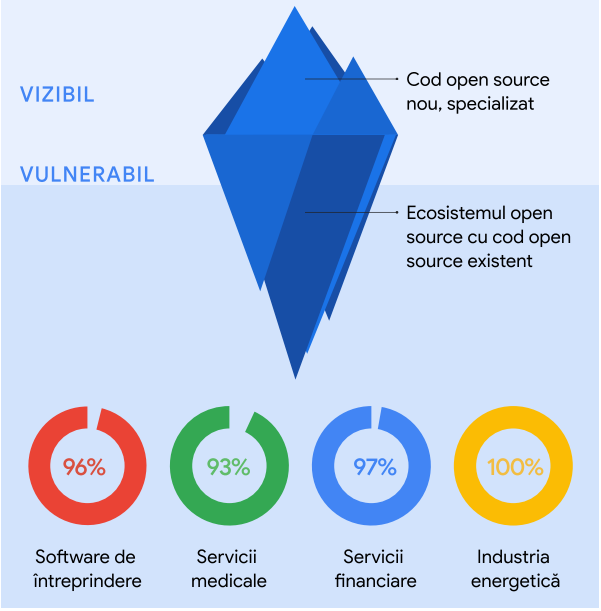
Comunitatea de dezvoltare open source, construită pe baza transparenței și "a permiterii accesului comun, contribuie cu un volum enorm de cod la majoritatea aplicațiilor pe care le utilizăm în prezent. De la echipamente medicale la rețeaua electrică, oamenii se bazează, practic, pe software din surse deschise (OSS) în fiecare oră din fiecare zi, ceea ce face proiectele din surse deschise o țintă preferată pentru atacurile cibernetice. În ultimii trei ani, s-a înregistrat o creștere de 742% de la un an la altul[1] a atacurilor asupra lanțului de aprovizionare software.

Ecosistemul open source este intrinsec structurat pe straturi, în care dependențele indirecte ascunse pot conține breșe de securitate. Aceste straturi fac vulnerabilitățile greu de detectat manual, iar securizarea acestei părți din dezvoltarea software a devenit o problemă de securitate urgentă la nivel global.

Este nevoie de o concentrare mai mare la toate nivelurile:

- Dezvoltatorii open source au nevoie de cunoștințe și de resurse pentru a-și securiza proiectele
- Organizațiile trebuie să înțeleagă riscurile și vulnerabilitățile lanțului de aprovizionare, pentru a dezvolta planuri de diminuare
- Autoritățile guvernamentale și industria trebuie să colaboreze pentru a asigura standarde de securitate solide și eficiente[3]

PROCENTUL DE SOFTWARE DIN INDUSTRIE CARE CONȚINE COD OPEN SOURCE[2]



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

Soluția noastră

Securizarea software-ului open source pentru toată lumea

La Google, lucrăm de ani întregi pentru a soluționa această problemă. De fapt, în fiecare an, peste 10% dintre utilizatorii Google contribuie la proiecte software open source. Pe baza experienței noastre, putem să concluzionăm că securitatea digitală modernă poate proveni, de fapt, din adoptarea deschiderii. Abordările deschise asigură posibilitatea de a adopta rapid cele mai recente inovații și de a permite mai multor oameni să rezolve problemele cibernetice. Dar, pentru deblocarea întregului potențial de valoare open source, avem nevoie de parteneriate public-privat mai puternice și de cadre de lucru create prin politici mai dinamice, pentru a oferi securitate tuturor. De aceea, salutăm eforturile făcute de guvernul S.U.A. de a dezvolta securitatea OSS, cum ar fi Legea privind securizarea software-ului open source (Securing Open Source Software Act), pusă în dezbatere în Senat, în 2022.

- Ne asumăm poziția de lider al comunității, cu cadre de lucru de următorul nivel în domeniul securității, cum ar fi nivelurile lanțului de aprovizionare pentru artefacte software - Supply-chain Levels for Software Artifacts (SLSA),[4,5] și dezvoltarea de instrumente de securitate avansate.
- Am elaborat un Grafic pentru înțelegerea compoziției artefactelor - Graph for Understanding Artifact Composition (GUAC), care aduce împreună informații de securitate software din diferite surse într-o singură bază de date, care poate fi interogată. GUAC va democratiza disponibilitatea informațiilor de securitate, prin disponibilitatea și posibilitatea de utilizare gratuită de către orice organizație.

Angajamentele noastre:

- Investiție de 100 de milioane de dolari în securitatea open source, roluri de lider în Fundația securității open source și colaborare directă cu dezvoltatorii
- Definirea și partajarea unor standarde de securitate aplicabile, a orientărilor, instrumentelor gratuite și bunelor practici pe care le utilizăm la nivel intern, cu întreaga comunitate open source
- Dezvoltarea detectării, trierea automată și modalitățile de a include securitatea în cele mai timpurii stadii de dezvoltare
- Automatizarea instrumentelor pentru ca securitatea de nivel corporativ să fie gratuită și accesibilă tuturor

Aplicații

Google OSS Fuzz
Răspunsul nostru la eroarea Heartbleed

Acea eroare Heartbleed a fost o vulnerabilitate din surse deschise gravă, o slăbiciune cu potențial de a afecta toți utilizatorii internetului. În 2014, hackerii au furat numele, adresele, datele de naștere, numerele de telefon și numerele de asigurări sociale a ~4,5 milioane de pacienți din baza de date a unuia dintre cele mai mari spitale din S.U.A.

Ca răspuns, Google a lansat OSS-Fuzz, ca serviciu comunitar gratuit. Testarea Fuzz identifică, în câteva minute, vulnerabilitățile de securitate necunoscute, spre deosebire de testarea manuală, care poate necesita luni întregi. Am investit în construirea unei infrastructuri pentru a testa automat sute de proiecte open source. OSS-Fuzz realizează acum scanări regulate ale codurilor și se inovează în permanență, pentru a găsi mai multe clase de erori.

Sunt scanate peste 800 de proiecte critice open source, prin testarea Fuzz în șase limbi.

Investițiile noastre în industrie și momentele semnificative

2020 — AUGUST
Am intrat în Fundația securității surselor deschise - Open Source Security Foundation (OpenSSF), pentru a ghida și îmbunătăți securitatea software-ului open source.

2021 — MAI ȘI IUNIE
Am stabilit bunele practici OSS în conformitate cu **Ordinul executiv al Casei Albe 14028** și am contribuit la orientările privind standardele de securitate ale lanțului de aprovizionare software.

2021 — IUNIE
Am lansat SLSA cu OpenSSF, externalizând cadrul de lucru intern Google în domeniul securității și permițând tuturor să construiască software mai securizat.

2021 — AUGUST
Ne-am angajat să investim 100 de milioane de dolari pentru a dezvolta și securiza OSS, inclusiv prin parteneriate cu dezvoltatori, pentru a găsi și remedia vulnerabilitățile.

2022 — MAI
Am anunțat Echipa Google pentru întreținerea open source, în timpul unei **Reuniuni la Washington, DC,** dedicând o echipă de dezvoltatori cu normă întreagă care să lucreze direct cu proiectele din surse deschise, pentru a le îmbunătăți securitatea.

2022 — MAI
Am anunțat produsul Software open source asigurat, care ajută la încorporarea acelorași pachete din surse deschise de încredere pe care Google le utilizează în fluxurile de lucru ale dezvoltatorilor.

Practicile recomandate de Google, care pot ajuta organizațiile publice și private să rămână în siguranță astăzi:

- Implementarea SLSA, pentru a întări securitatea lanțului de aprovizionare software
- Semnătura criptografică și verificarea autenticității software-ului, folosind Sigstore
- Descoperirea, urmărirea și trierea automată a vulnerabilităților, cu OSS-Fuzz și OSV.dev
- Utilizarea fișelor de evaluare, pentru a evalua automat riscurile de securitate cu dependențele tale

Abordarea noastră

Software-ul este securizat doar dacă până și ultima sa verigă este securizată. Investim experiența și resursele noastre financiare pentru a crește securitatea întregului ecosistem din surse deschise. Echipa noastră de dezvoltare și experții în securitate cred că putem proteja mai multe organizații publice și private, în următoarele moduri:

Echipa noastră auditează fiecare stadiu al ciclului de viață al produsului, scanând, analizând și testând fuzz în permanență, pentru a identifica vulnerabilitățile

Susținem internetul deschis, partajând ceea ce știm cu comunitatea de dezvoltatori și asigurând securitatea acestuia pentru public și firme

Pregătim securitatea viitorului prin detectarea amenințărilor sofisticate, asigurarea instrumentelor automate avansate și intuirea a ceea ce urmează

Securizarea software-ului open source este o responsabilitate comună și ne asumăm continuarea colaborării în această problemă critică, urgentă.
g.co/security/gosst

Surse: 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. Partajarea cunoștințelor noastre (mai exact, lansarea SLSA, ghidarea OpenSSF) înseamnă că oricine creează software, nu doar Google, poate beneficia de experiența și de practicile de securitate ale Google, testate în timp. 5. SLSA este un set de practici care pot ajuta organizațiile să își îmbunătățească securitatea și procesul de dezvoltare a software-ului. Ajută la respectarea Cadrului de lucru pentru dezvoltarea software securizată al guvernului S.U.A., cerințe stabilite de autoritățile guvernamentale ca răspuns la Ordinul executiv privind securitatea cibernetică. Aceasta înseamnă că organizațiile vor beneficia de îndrumare privind modalitățile de a respecta orientările federale, pentru ca software-ul să fie mai sigur pentru toată lumea.