Sikring af grundlaget for softwareudvikling

Med den dramatiske stigning i statsfinansierede cyberangreb og ondsindede onlineaktører, mener vi, at vores produkter og tjenester kun er så nyttige, som de er sikre. Hos Google er vi mere fokuserede end nogensinde på at beskytte mennesker, organisationer og regeringer ved at dele vores ekspertise, så vi kan gøre samfundet i stand til at håndtere cyberrisici, som hele tiden udvikles, og løbende arbejde for at forbedre det ypperste inden for cybersikkerhed for at skabe en sikrere verden for alle.

Open source-software – kode, der stilles frit til rådighed for alle at bruge, ændre og bygge videre på – er grundlaget for det moderne internet. Verden inden for open source-softwareudvikling tillader samarbejde og hurtig innovation ved frit at dele løsninger. Dog gør netop den åbenhed, der gør den digitale verden tilgængelig for alle, den unikt sårbar over for sikkerhedstrusler.

Udfordring

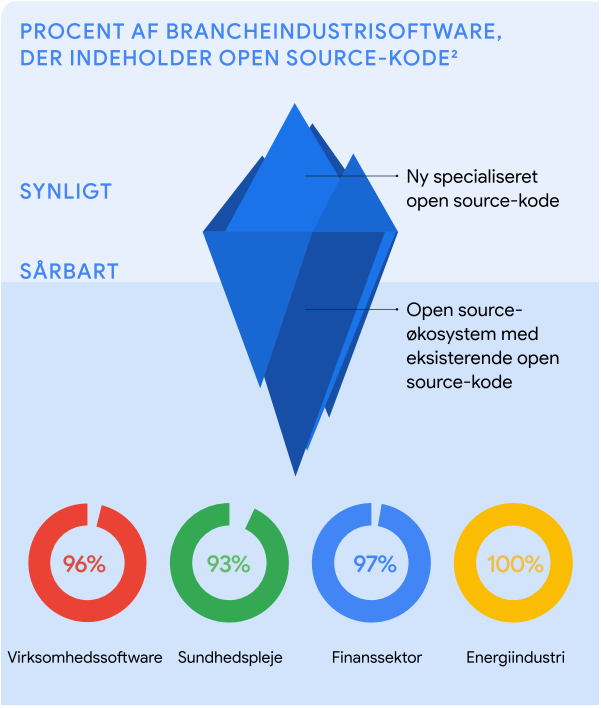
Open source-software vedrører alle

Open source-udviklingsfællesskabet, som er bygget på gennemsigtighed og deling, bidrager med en enorm mængde kode til de fleste applikationer, vi bruger i dag. Lige fra medicinsk udstyr til elnettet er folk afhængige af open source-software (OSS) stort set hver time hver dag – hvilket gør open source-projekter til et primært mål for cyberangreb. Der har de sidste tre år været en stigning i angreb i softwareforsyningskæden på 742 % fra år til år[1].

Open source-økosystemet er lagdelt på en kompliceret måde, hvor skjulte indirekte afhængigheder kan indeholde sikkerhedsbrister. Disse lag gør sårbarheder svære at opdage manuelt, og sikring af denne del af softwareudvikling er blevet et presserende globalt sikkerhedsproblem.

Der er behov for yderligere fokus på alle niveauer:

- Open source-udviklere har brug for viden og ressourcer for at sikre deres projekter
- Organisationer er nødt til at forstå risici og sårbarheder i forsyningskæden for at udvikle afværgeplaner
- Regeringer og brancheindustrien må samarbejde for at sikre robuste, effektive sikkerhedsstandarder[3]



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

Vores løsning

Sikring af open source-software for alle

Hos Google har vi arbejdet på denne udfordring i årevis. Faktisk bidrager over 10 % af medarbejderne hos Google hvert år til open source-softwareprojekter. Vores erfaring får os til at konkludere, at moderne digital sikkerhed faktisk kan opnås ved at omfavne åbenhed. En åben tilgang sikrer, at vi hurtigt kan adoptere de nyeste innovationer og give flere mennesker mulighed for at løse sikkerhedsudfordringer. Men for at frigøre den fulde værdi af open source har vi brug for stærkere offentlig-private partnerskaber og dynamiske politiske rammer for at styrke sikkerheden for alle. Derfor hilser vi den amerikanske regerings indsats for at fremme OSS-sikkerhed velkommen, f.eks. Securing Open Source Software Act, der blev indført i Senatet i 2022.

- Vi leder fællesskabet med sikkerhedsrammer på næste niveau, f.eks. Supply-chain Levels for Software Artifacts (SLSA),[4,5] og udvikling af avancerede sikkerhedsværktøjer.
- Vi har udviklet Graph for Understanding Artifact Composition (GUAC), som samler softwaresikkerhedsoplysninger fra forskellige kilder i en enkelt forespørgelig database. GUAC vil demokratisere tilgængeligheden af sikkerhedsoplysninger ved at gøre dem frit tilgængelige og nyttige for enhver organisation.

Vi forpligter os til at:

- Investere 100 millioner USD i open source-sikkerhed, have lederroller i Open Source Security Foundation og samarbejde direkte med udviklere
- Definere og dele handlingsrettede sikkerhedsstandarder, vejledning, gratis værktøjer og den bedste praksis vi bruger internt med hele open source-fællesskabet
- Accelerere sporing, automatiseret triagering og måder at bygge sikkerhed på i de tidligste udviklingsstadier
- Automatisere værktøjer for at gøre sikkerhed på virksomhedsniveau gratis og tilgængelig for alle

Applikationer

Google OSS Fuzz
Vores svar på the Heartbleed bug

The Heartbleed bug var en alvorlig open source-sårbarhed og en svaghed med potentiale til at påvirke næsten alle internetbrugere. I 2014 stjal hackere navne, adresser, fødselsdatoer, telefonnumre og personnumre i et antal svarende til 4,5 millioner patienter fra databasen på et af de største amerikanske hospitaler

Som modsvar lancerede Google OSS-Fuzz som en gratis samfundstjeneste. Fuzz-test lokaliserer ukendte sikkerhedssvagheder på få minutter, i modsætning til manuelle test, som kan tage måneder. Vi investerede i at bygge en infrastruktur til automatisk at teste hundredvis af open source-projekter. OSS-Fuzz udfører nu regelmæssige kodescanninger og udvikler sig konstant for at finde flere fejlklasser.

Der er scannet mere end 800 kritiske open source-projekter, hvor Fuzz har testet på seks sprog.

Vores brancheinvesteringer og milepæle

2020 – AUGUST
Tiltrådte Open Source Security Foundation (OpenSSF) for at vejlede og forbedre sikkerheden i open source-software.

2021 – MAJ OG JUNI
Etablerede bedste praksis for OSS i overensstemmelse med **Det Hvide Hus' bekendtgørelse 14028** og bidrog med vejledning om sikkerhedsstandarder for softwareforsyningskæden.

JUNI
Frigav SLSA med OpenSSF, der eksternaliserer Googles interne sikkerhedsramme og giver alle mulighed for at bygge mere sikker software.

AUGUST
Garanterede 100 millioner USD til at løfte og sikre OSS, herunder samarbejde med udviklere for at finde og rette sårbarheder.

2022 – MAJ
Annoncerede Googles Open Source Maintenance Crew under et **Washington DC Summit,** der dedikerede et team af fuldtidsudviklere til at arbejde direkte med open source-projekter for at forbedre deres sikkerhed.

MAJ
Annoncerede Assured Open Source Software-produktet, som hjælper med at inkorporere de samme sikre open source-pakker, som Google bruger i udviklerarbejdsgange.

Googles anbefalede praksis, der i dag kan hjælpe offentlige og private organisationer med at forblive sikre:

- Implementer SLSA for at styrke sikkerheden i softwareforsyningskæden
- Underskriv kryptografisk og verificer ægtheden af din software ved hjælp af Sigstore
- Automatiser sårbarhedsopdagelse, sporing og triagering med OSS-Fuzz og OSV.dev
- Brug Scorecards til automatisk at evaluere sikkerhedsrisici med dine afhængigheder

Vores tilgang

Software er kun lige så sikker som det svageste led. Vi investerer vores ekspertise og finansielle ressourcer for at øge sikkerheden i hele open source-økosystemet. Vores team af udviklings- og sikkerhedseksperter mener, at vi kan beskytte flere offentlige og private organisationer på følgende måder:

Vores team gennemgår hvert trin i produktets livscyklus, scanner, analyserer og fuzz-tester for sårbarheder

Vi støtter det åbne internet og deler det, vi ved, med udviklerfællesskabet og holder det sikkert for offentligheden og virksomhederne

Vi fremtidssikrer ved at detektere sofistikerede trusler, levere avanceret automatiseret værktøj og være et skridt foran, hvad end det næste bliver

Sikring af open source-software er et fælles ansvar, og vi er forpligtet til fortsat samarbejde om dette presserende, kritiske problem. g.co/security/gosst

Kilder: 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. At dele vores viden (dvs. frigive SLSA og vejlede i OpenSSF) betyder, at alle, der udvikler software, ikke kun Google, kan drage fordel af Googles erfaring og gennemtestede sikkerhedspraksis. 5. SLSA er et sæt af praksis, der kan hjælpe organisationer med at forbedre sikkerheden i deres softwareudviklingsproces. Det hjælper med at opfylde den amerikanske regerings Secure Software Development Framework, som er krav fastsat af regeringen som svar på bekendtgørelsen om cybersikkerhed. Det betyder, at organisationer vil få vejledning i, hvordan de overholder føderale retningslinjer for at gøre software mere sikker for alle.