En säker grund för programvaruutveckling

Med den drastiska ökningen i antalet statsstödda cyberattacker och skadliga aktörer online anser vi att våra produkter och tjänster är mer användbara ju säkrare de är. Vi på Google fokuserar mer än någonsin på att skydda personer, organisationer och myndigheter genom att dela med oss av våra expertkunskaper, göra det möjligt för samhället att ta itu med ständigt föränderliga cyberrisker och hela tiden arbeta på att utveckla det senaste inom cybersäkerhet så att vi kan göra världen till en tryggare plats för alla.

Öppna programvaror, det vill säga programvaror med kod som alla får använda, ändra och bygga vidare på, är grunden för dagens internet. När man utvecklar öppna programvaror finns det plats för samarbete och snabb innovation eftersom lösningar sprids fritt. Det är dock just öppenheten, den som gör den digitala världen tillgänglig för alla, som gör den extra utsatta för säkerhetshot.

Utmaning

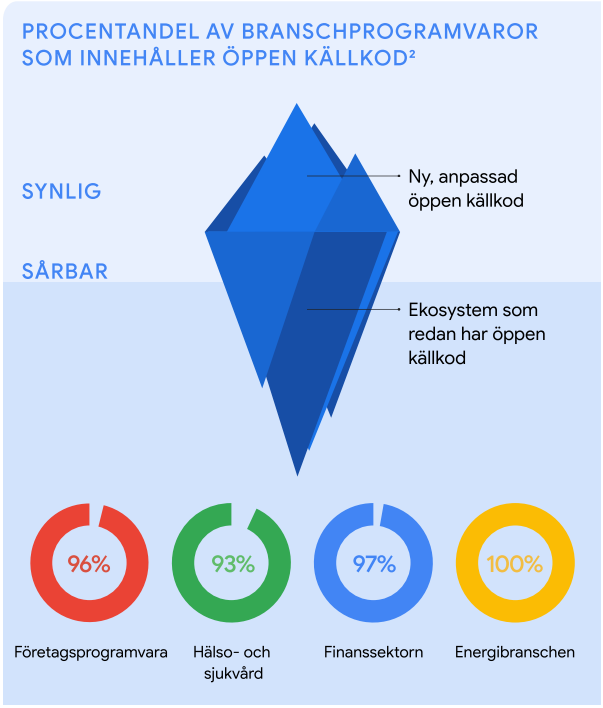
Öppna programvaror är ett problem för alla

Utvecklingsgemenskapen som tar fram öppen källkod sätter insyn och delning i centrum och tillhandahåller en stor mängd kod till de flesta appar som vi använder just nu. Människor förlitar sig på öppna programvaror i allt från medicinsk utrustning till elnätet alla dygnets timmar. Det gör projekt med öppen källkod till väldigt intressanta mål att attackera. Under de senaste tre åren har attacker på distributionskedjor av programvaror ökat med 742 procent jämfört med föregående år[1].

Ekosystemet med öppen källkod är uppbyggt med flera invecklade lager där gömda indirekta beroenden kan ha säkerhetsbrister. På grund av de här lagren är det svårt att upptäcka säkerhetsrisker manuellt, och det har blivit viktigt globalt sett att skydda den här delen av programvaruutveckling.

Större fokus krävs på alla nivåer:

- Utvecklare av öppen källkod behöver kunskap och resurser för att kunna skydda sina projekt.
- Organisationer behöver ha koll på de risker och brister som finns i distributionskedjan så att de kan ta fram åtgärdsplaner.
- Myndigheter och branschfolk måste tillsammans ta fram robusta och effektiva säkerhetsstandarder[3].



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

Vår lösning

Skydda programvaror med öppen källkod för alla

Vi har jobbat med det här i många år på Google. Det är faktiskt så att fler än 10 procent av de anställda hos Google bidrar till projekt med öppna programvaror. Utifrån vår erfarenhet tänker vi att vi kan få modern digital säkerhet genom att vara öppna. Genom att använda öppen källkod kan vi snabbt komma igång och använda nya innovationer och ge fler möjligheten att lösa säkerhetsproblem. Men vi kan få ut ännu mer av öppen källkod. Vi behöver därför starkare samarbeten mellan det offentliga och privata samt dynamiska policyramverk så att vi kan öka säkerheten för alla. Därför är vi glada över att USA:s regering arbetar för att förstärka säkerheten för öppna programvaror, bland annat genom Securing Open Source Software Act som röstades igenom av senaten 2022.

- Vi hjälper också gruppen genom att ta fram mer avancerade säkerhetsramverk, som Supply-chain Levels for Software Artifacts (SLSA)[4,5], och genom att utveckla avancerade säkerhetsverktyg.
- Vi tog fram Graph for Understanding Artifact Composition (GUAC), som samlar information om programvarusäkerhet från olika källor i en enda databas som man kan söka i. GUAC demokratiserar tillgängligheten på säkerhetsinformation eftersom informationen blir helt tillgänglig och kan användas av alla organisationer.

Våra åtaganden:

- Investera 100 miljoner US-dollar i säkerhet för öppen källkod, ledningsroller i Open Source Security Foundation och direkt samarbete med utvecklare.
- Definiera och dela säkerhetsstandarder med åtgärder, vägledning och kostnadsfria verktyg och tips som vi använder internt med hela gruppen för öppen källkod.
- Utveckla avancerade identifieringsfunktioner, automatiserad utvärdering och sätt att bygga in säkerhet så tidigt som möjligt i utvecklingsprocessen.
- Automatisera verktyg så att skydd på företagsnivå blir kostnadsfritt och tillgängligt för alla.

Appar

Google OSS Fuzz
Vårt svar på Heartbleed-buggen

Heartbleed-buggen var en allvarlig säkerhetsrisk i öppen källkod, en brist som hade kunnat påverka nästan alla internetanvändare. År 2014 stal hackare ungefär 4,5 miljoner patienters namn, adresser, födelsedatum, telefonnummer och personnummer från databasen för ett av de största sjukhusen i USA.

På grund av detta lanserade Google OSS-Fuzz som en kostnadsfri samhällstjänst. Med Fuzz-tester kan man upptäcka okända säkerhetsbrister på bara några minuter, som annars kan ta månader när man testar manuellt. Vi har byggt upp en infrastruktur så att vi automatiskt kan testa hundratals projekt med öppen källkod. OSS-Fuzz genomsöker nu regelbundet kod och utvecklas hela tiden så att fler buggklasser ska kunna hittas.

Fler än 800 viktiga projekt med öppen källkod söks igenom med Fuzz-tester på sex språk.

Våra investeringar i branschen och milstolpar

2020 – AUGUSTI
Gick med i Open Source Security Foundation (OpenSSF) för att vägleda och förbättra säkerheten i öppna programvaror.

2021 – MAJ OCH JUNI
Etablerade bästa metoder för öppna programvaror i enlighet med **Vita husets exekutiva order 14028** och bidrog med information om säkerhetsstandarder för distributionskedjan av programvaror.

JUNI
Släppte SLSA med OpenSSF, så att Googles interna säkerhetsramverk blev tillgängligt för andra utanför Google och alla fick möjlighet att skapa säkrare programvaror.

AUGUSTI
Dedikerade 100 miljoner US-dollar på att uppgradera och säkra öppna programvaror, bland annat genom partnerskap med utvecklare som kan hitta och fixa säkerhetsrisker.

2022 – MAJ
Lanserade Googles Open Source Maintenance Crew under en **DC Summit,** vilket är ett särskilt team med heltidsanställda utvecklare som ska jobba direkt med att förbättra säkerheten för projekt med öppen källkod.

MAJ
Presenterade produkten Assured Open Source Software, som gör det enklare att implementera samma betrodda paket med öppen källkod som Google använder i utvecklares arbetsflöden.

Rekommenderade metoder av Google som kan hjälpa offentliga och privata organisationer att skydda sig redan nu:

- Implementera SLSA så att distributionskedjan för programvaror blir säkrare
- Signera och verifiera programvaran kryptografiskt med Sigstore.
- Automatisera identifiering, spårning och utvärdering av säkerhetsrisker med OSS-Fuzz och OSV.dev.
- Använd Scorecard till att automatiskt bedöma säkerhetsrisken för dina beroenden.

Vår metod

Ingen programvara är säkrare än dess svagaste länk. Vi lägger våra expertkunskaper och ekonomiska resurser på att öka säkerheten i hela ekosystemet med öppen källkod. Vårt team med utvecklings- och säkerhetsexperter är övertygade om att vi kan skydda fler offentliga och privata organisationer på följande sätt:

Vårt team granskar varenda steg i produktens livscykel och genomsöker, analyserar och utför Fuzz-tester löpande på jakt efter säkerhetsrisker.

Vi stöttar nätneutralitet genom att dela vår kunskap med utvecklargemenskapen och hålla internet säkert för allmänheten och företag.

Vi framtidssäkrar säkerheten genom att identifiera avancerade hot, tillhandahålla avancerade och automatiserade verktyg och ligga steget före.

Vi har ett gemensamt ansvar att skydda öppna programvaror, och vi strävar efter att fortsätta att samarbeta för att lösa det här brådskande, viktiga problemet. g.co/security/gosst

Källor: 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. Vi delar med oss av vår kunskap (bland annat genom att släppa SLSA och vägleda OpenSSF). Det innebär att alla som skapar programvara, inte bara Google, kan dra nytta av Googles erfarenhet och beprövade säkerhetsmetoder. 5. SLSA består av en rad metoder som kan underlätta för organisationer när de ska förbättra säkerheten i processen för programvaruutveckling. Det blir på så sätt enklare att uppfylla kraven i USA:s regerings ramverk om säker programvaruutveckling, krav som myndigheterna tog fram på grund av den exekutiva ordern om cybersäkerhet. Det innebär att organisationer får information om vad de ska göra för att uppfylla federala riktlinjer så att programvaror blir säkrare för alla.