De basis voor softwareontwikkeling veilig maken

Met de dramatische toename van staatsgesponsorde hackersaanvallen en kwaadwillende individuen online, vinden we dat onze producten en diensten alleen nuttig zijn als ze echt veilig zijn. Bij Google zijn we er meer dan ooit op gericht mensen, organisaties en overheden te beschermen door onze expertise te delen, de samenleving de middelen te geven om de steeds evoluerende digitale risico's aan te pakken en ons voortdurend in te zetten voor de bescherming van mensen en overheden, en voortdurend te werken aan verbetering van de stand van de techniek op het gebied van cybersecurity om zo een veiligere wereld voor iedereen te realiseren.

Opensourcesoftware – code die voor iedereen vrij beschikbaar is om te gebruiken, aan te passen en op voort te bouwen – is de basis van het moderne internet. De wereld van opensourcesoftwareontwikkeling maakt samenwerking en snelle innovatie mogelijk doordat oplossingen vrijelijk worden gedeeld. Maar juist die openheid waardoor de digitale wereld voor iedereen toegankelijk is, maakt haar ook bijzonder kwetsbaar voor veiligheidsinbreuken.

Uitdaging

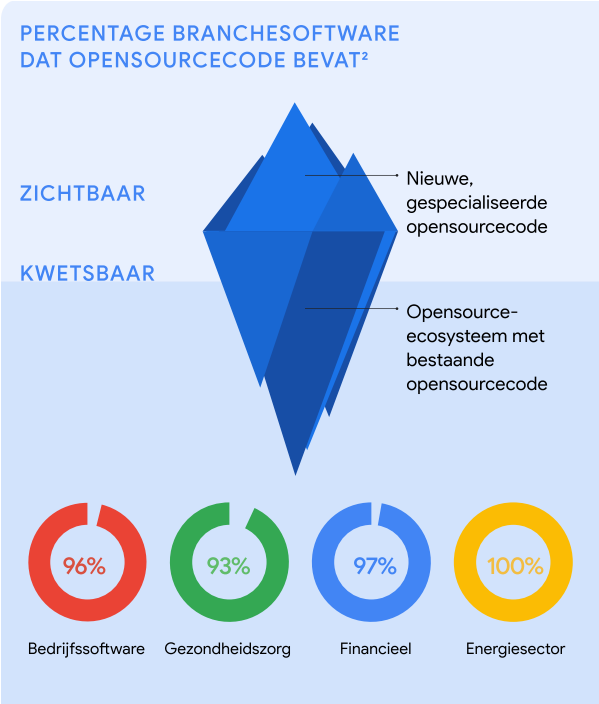
Opensourcesoftware gaat iedereen aan

De op transparantie en met elkaar delen gestoelde opensource-ontwikkelingsgemeenschap heeft een enorme hoeveelheid code bijgedragen aan de meeste toepassingen die we tegenwoordig gebruiken. Of het nu gaat om medische apparatuur of het elektriciteitsnet, mensen vertrouwen vrijwel elk uur van de dag op opensourcesoftware (OSS), waardoor opensourceprojecten een belangrijk doelwit zijn voor cyberaanvallen. In de afgelopen drie jaar zagen we **jaar-op-jaar een toename van 742%**[1] het aantal aanvallen op de leveringsketen van software.

Het opensource-ecosysteem heeft een ingewikkelde gelaagdheid, waarbij verborgen indirecte afhankelijkheden veiligheidslekken kunnen bevatten. Door deze gelaagdheid zijn kwetsbaarheden nauwelijks handmatig op te sporen en de beveiliging van dit deel van softwareontwikkeling vormt inmiddels wereldwijd een urgent beveiligingsprobleem.

Op alle niveaus is extra aandacht vereist:

- Opensourceontwikkelaars hebben de kennis en middelen nodig om hun projecten te beveiligen
- Organisaties moeten begrijpen wat de risico's en kwetsbaarheden van de toeleveringsketen zijn om plannen voor risicobeperking te kunnen ontwikkelen
- Overheden en het bedrijfsleven moeten samenwerken om robuuste, doeltreffende beveiligingsnormen te waarborgen[3]



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

Onze oplossing

Opensourcesoftware voor iedereen veilig maken

Bij Google werken we al jaren aan deze uitdaging. In werkelijkheid draagt elk jaar meer dan 10% van de gebruikers van Google bij aan opensourcesoftwareprojecten. Onze ervaring leert ons dat moderne digitale veiligheid juist door openstaan voor openheid kan worden bereikt. Door een open aanpak kunnen we de nieuwste innovaties snel invoeren zodat meer mensen beveiligingsproblemen kunnen oplossen. Maar om de waarde van open source volledig te benutten, hebben we sterkere publiek-private partnerschappen en dynamische beleidskaders nodig om de veiligheid voor iedereen te versterken. Om die reden verwelkomen we de inspanningen van de Amerikaanse overheid om de beveiliging van OSS te bevorderen, zoals de in 2022 in de Senaat ingediende Securing Open Source Software Act.

- We nemen het voortouw in de gemeenschap met next-level beveiligingskaders, zoals Supply-chain Levels for Software Artifacts (SLSA),[4,5] en ontwikkelen geavanceerde beveiligingsinstrumenten.
- Graph for Understanding Artifact Composition (GUAC) hebben we ontwikkeld om informatie over softwarebeveiliging uit verschillende bronnen samen te brengen in één doorzoekbare database. GUAC zal de beschikbaarheid van beveiligingsinformatie democratiseren door het vrij toegankelijk te maken voor elke organisatie.

Onze commitments:

- 100 miljoen dollar investeren in opensourcebeveiliging, de voortrekkersrol nemen in de Open Source Security Foundation en directe samenwerking met ontwikkelaars
- De actiegerichte beveiligingsnormen, richtlijnen, kosteloze tools en beste praktijken die we intern gebruiken definiëren en delen met de hele opensourcegemeenschap
- Geavanceerde detectie, geautomatiseerde triage en manieren om beveiliging al in de vroegste ontwikkelingsstadia in te bouwen
- Automatiseren van tooling om beveiliging op bedrijfsniveau kosteloos en voor iedereen toegankelijk te maken

Toepassingen

Google OSS Fuzz

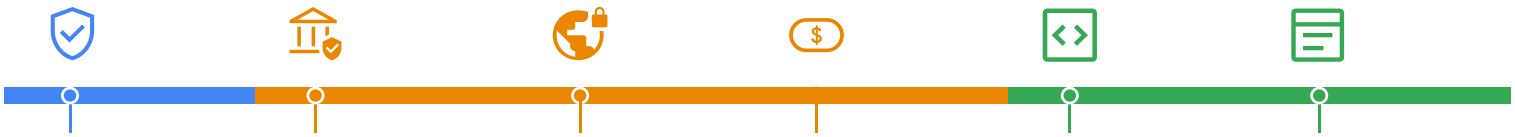
Ons antwoord op de Heartbleed-bug

De Heartbleed bug was een ernstige opensourcekwetsbaarheid, een zwak punt dat bijna elke internetgebruiker kon treffen. In 2014 stalen hackers de namen, adressen, geboortedata, telefoonnummers en socialezekerheidnummers van ± 4,5 miljoen patiënten uit de database van een van de grootste Amerikaanse ziekenhuizen.

Als antwoord daarop lanceerde Google OSS-Fuzz als kosteloze dienst voor de gemeenschap. In tegenstelling tot handmatig testen, dat maanden kan duren, identificeert fuzz testing binnen enkele minuten onbekende zwakke plekken in de beveiliging. We hebben geïnvesteerd in het bouwen van een infrastructuur om honderden opensourceprojecten automatisch te kunnen testen. OSS-Fuzz voert nu regelmatig codescans uit en innoveert continu om meer bugklasses te vinden.

800+ cruciale opensourceprojecten in zes talen zijn door Fuzz testing gescand.

Onze branche-investeringen en mijlpalen



2020 — AUGUSTUS

Toetreding tot de Open Source Security Foundation (OpenSSF) om de veiligheid van opensourcesoftware te begeleiden en te verbeteren

2021 — MEI EN JUNI

Vaststelling van de beste OSS-praktijken in overeenstemming med **White House Executive Order 14028** en bijdragen aan richtlijnen voor beveiligingsnormen voor de softwareketen.

JUNI

Uitbrengen van SLSA met OpenSSF, waarmee het interne beveiligingsraamwerk van Google wordt geëxternaliseerd en iedereen veiligere software kan maken.

AUGUSTUS

Toezegging van meer dan 100 miljoen dollar om OSS te verbeteren en beveiligen, waarbij wordt samengewerkt met ontwikkelaars om kwetsbaarheden op te sporen en te verhelpen

2022 — MEI

Aankondiging van Google's Open Source Maintenance Crew tijdens een DC Summit, waarbij een team van fulltime ontwikkelaars rechtstreeks met opensourceprojecten werkt om hun beveiliging te verbeteren.

MEI

Aankondiging van het Assured Open Source Software-product, dat helpt dezelfde vertrouwde opensourcepakketten waar Google gebruik van maakt op te nemen in de workflows van ontwikkelaars.

De door Google aanbevolen praktijken die publieke en particuliere organisaties vandaag kunnen helpen veilig te blijven:

- Implementeer SLSA om de beveiliging van de leveringsketen van software te versterken
- Gebruik Sigstore voor cryptografisch ondertekenen en om de authenticiteit van je software verifiëren
- Automatiseer het opsporen, traceren en verhelpen van kwetsbaarheden met OSS-Fuzz en OSV.dev
- Gebruikmaken van scorecards waarmee je automatisch het beveiligingsrisico van je afhankelijkheden evalueert

Onze aanpak

Software is zo veilig als de zwakste schakel. We investeren onze expertise en financiële middelen om de veiligheid van het hele opensource-ecosysteem te verbeteren. Ons team van ontwikkelings- en beveiligingsdeskundigen is van oordeel dat we meer publieke en particuliere organisaties op de volgende manieren kunnen beschermen:

Ons team controleert elke fase van de productlevenscyclus en scant, analyseert en doet fuzztests om kwetsbaarheden op te sporen

We ondersteunen het open internet, delen wat we weten met de ontwikkelaarsgemeenschap en houden het veilig voor publiek en bedrijven

Door geavanceerde dreigingen te detecteren, geavanceerde geautomatiseerde tools te bieden en altijd een stap vooruit te zijn, maken we beveiliging toekomstbestendig

Het beveiligen van opensourcesoftware is een gedeelde verantwoordelijkheid en daarom willen we blijven samenwerken aan dit urgente, kritieke **probleem.** g.co/security/gosst

Voetnoten: 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. Het delen van onze kennis (dat wil zeggen het uitbrengen van SLSA en het begeleiden van OpenSSF) betekent dat niet alleen Google, maar iedereen die software maakt, kan profiteren van de ervaring en beproefde beveiligingspraktijken van Google, 5. De SLSA bestaat uit een aantal praktijken waarmee organisaties de veiligheid van hun softwareontwikkelingsproces kunnen verbeteren. Het helpt om te kunnen voldoen aan het Secure Software Development Framework van de Amerikaanse overheid, voorschriften die de overheid heeft opgesteld in reactie op het uitvoeringsbesluit inzake cyberveiligheid. Dat betekent dat organisaties begeleiding krijgen met betrekking tot hoe ze kunnen voldoen aan de federale richtlijnen om software voor iedereen veiliger te maken.