Zabezpečení základů pro vývoj softwaru

Vzhledem k dramatickému nárůstu kybernetických útoků sponzorovaných státy a záškodníků na internetu jsme přesvědčeni, že naše produkty a služby jsou jen tak užitečné, jak jsou bezpečné. Proto se v Googlu nyní víc než dřív zaměřujeme na ochranu lidí, organizací a vlád. Sdílíme své odborné znalosti, pomáháme společnosti čelit neustále se vyvíjejícím kybernetickým rizikům, snažíme se zvyšovat kybernetickou bezpečnost a vytvářet bezpečnější svět pro všechny.

Základem moderního internetu je software s otevřeným zdrojovým kódem, který je volně k dispozici, aby jej mohl kdokoli používat, upravovat ho a stavět na něm. Svět vývoje softwaru s otevřeným zdrojovým kódem umožňuje spolupráci a rychlé inovace díky volnému sdílení řešení. Tato otevřenost, díky níž je digitální svět přístupný všem, však s sebou nese zranitelnost vůči bezpečnostním hrozbám.

Problém

Starost o software s otevřeným zdrojovým kódem se týká všech

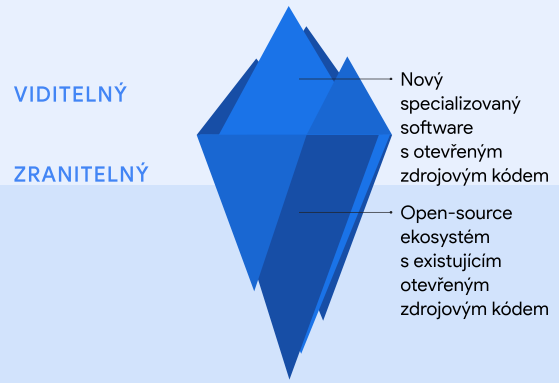
Komunita vývojářů open source, založená na transparentnosti a sdílení, přispívá obrovským množstvím kódu k většině aplikací, které dnes používáme. Lidé se prakticky každou hodinu spoléhají na software s otevřeným zdrojovým kódem (OSS) – od lékařských přístrojů až po rozvodnou síť – a proto jsou projekty s otevřeným zdrojovým kódem hlavním cílem kybernetických útoků. V posledních třech letech došlo k meziročnímu nárůstu útoků na dodavatelský řetězec softwaru o 742 %[1].

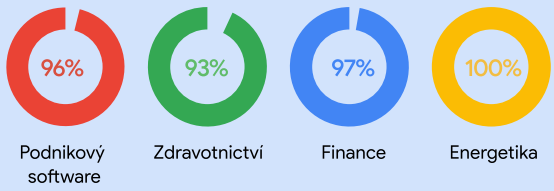
Ekosystém open source je složitě vrstvený a skryté nepřímé závislosti mohou obsahovat bezpečnostní chyby. Kvůli této vrstevnatosti je obtížné odhalit zranitelnosti ručně a ze zabezpečení této části vývoje softwaru se tak stal naléhavý bezpečnostní problém na celém světě.

Je třeba mu věnovat pozornost na všech úrovních:

- Vývojáři open source potřebují znalosti a zdroje pro zabezpečení svých projektů
- Organizace musí porozumět rizikům a zranitelným místům v dodavatelském řetězci, aby mohly vypracovat plány na jejich zmírnění
- Vlády a firmy musí spolupracovat na zajištění spolehlivých a účinných bezpečnostních norem[3]

PROCENTO SOFTWARU, KTERÝ OBSAHUJE OTEVŘENÝ ZDROJOVÝ KÓD[2]





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

Naše řešení

Zabezpečit software s otevřeným zdrojovým kódem pro všechny

V Googlu se tímto problémem zabýváme již několik let. Více než 10 % zaměstnanců společnosti Google každoročně přispívá do projektů softwaru s otevřeným zdrojovým kódem. Zkušenosti nás vedou k závěru, že moderní digitální bezpečnost lze skutečně zajistit právě skrze otevřenost. Díky otevřeným přístupům můžeme rychle přijímat nejnovější inovace a umožnit více lidem řešit bezpečnostní problémy. Abychom však plně využili hodnotu open source, potřebujeme silnější partnerství veřejného a soukromého sektoru a dynamické politické rámce, které zajistí bezpečnost pro všechny. Proto vítáme snahy americké vlády o posílení bezpečnosti OSS, jako je například návrh zákona o zabezpečení softwaru s otevřeným zdrojovým kódem, který byl v roce 2022 předložen v Senátu.

- Jsme lídrem komunity s vynikajícími bezpečnostními rámci, jako je rámec pro ochranu před útoky na dodavatelský řetězec softwaru Supply-chain Levels for Software Artifacts (SLSA),[4,5] a vyvíjíme pokročilé bezpečnostní nástroje.
- Vyvinuli jsme Graph for Understanding Artifact Composition (GUAC), který ukládá informace o zabezpečení softwaru z různých zdrojů do jediné databáze, v níž lze vyhledávat. GUAC bude demokratizovat dostupnost bezpečnostních informací tím, že je zpřístupní všem organizacím.

Zavazujeme se:

- Investovat 100 milionů dolarů do bezpečnosti open source, nadále vést nadaci Open Source Security Foundation a přímo spolupracovat s vývojáři
- Definovat a sdílet použitelné bezpečnostní standardy, pokyny, bezplatné nástroje a osvědčené postupy , které používáme interně, s celou open source komunitou
- Uspíšit detekci, automatizované třídění a způsoby, jak integrovat zabezpečení do nejranějších fází vývoje
- Automatizovat nástroje tak, aby zabezpečení na podnikové úrovni bylo bezplatné a každému dostupné

Aplikace

Google OSS-Fuzz

Naše reakce na bezpečnostní chybu Heartbleed

Bezpečnostní chyba Heartbleed byla závažná zranitelnost otevřeného zdroje, slabina s potenciálem ovlivnit téměř každého uživatele internetu. V roce 2014 ukradli hackeři z databáze jedné z největších amerických nemocnic jména, adresy, data narození, telefonní čísla a čísla sociálního pojištění přibližně 4,5 milionu pacientů.

V reakci na to Google spustil OSS-Fuzz jako bezplatnou komunitní službu. Na rozdíl od manuálního testování, které může trvat měsíce, fuzz testování odhalí neznámé slabiny zabezpečení během několika minut. Investovali jsme do vybudování infrastruktury pro automatické testování stovek projektů s otevřeným zdrojovým kódem. OSS-Fuzz nyní provádí pravidelné skenování kódu a neustále inovuje, aby našel další třídy chyb.

Pomocí fuzz testování v šesti jazycích se skenuje více než 800 zásadních open source projektů.

Naše investice a milníky v oboru

2020

SRPEN

Vstoupili jsme do nadace Open Source Security Foundation (OpenSSF) s cílem řídit a zlepšovat bezpečnost softwaru s otevřeným zdrojovým kódem.

2021

KVĚTEN A ČERVEN

Zavedli jsme osvědčené postupy OSS v souladu s exekutivním nařízením Bílého domu č. 14028 a pomohli jsme s přípravou bezpečnostních standardů dodavatelského řetězce softwaru.

ČERVEN

Vydali jsme SLSA s OpenSSF, čímž jsme externalizovali interní bezpečnostní rámec společnosti Google a umožnili všem vytvářet bezpečnější software.

SRPEN

Přislíbili jsme 100 milionů dolarů na posílení a zabezpečení OSS, včetně spolupráce s vývojáři při hledání a odstraňování zranitelností.

2022

KVĚTEN

Na summitu ve Washingtonu jsme oznámili vytvoření týmu vývojářů na plný úvazek, který bude přímo spolupracovat s projekty s otevřeným zdrojovým kódem a zlepšovat jejich zabezpečení.

KVĚTEN

Ohlásili jsme vznik produktu **Assured Open Source Software**, který pomáhá začlenit do pracovních postupů vývojářů stejné důvěryhodné open source balíčky, jaké používá společnost Google.

Společnost Google doporučila postupy, které mohou veřejným i soukromým organizacím pomoci zachovat bezpečnost:

- Implementovat SLSA pro posílení bezpečnosti dodavatelského řetězce softwaru
- Používat šifrované podepisování a ověřovat pravost softwaru pomocí aplikace Sigstore
- Automatizovat odhalování, sledování a odstraňování zranitelností pomocí OSS-Fuzz a OSV.dev
- Pomocí Scorecards automaticky vyhodnocovat bezpečnostní rizika u vašich zařízení

Náš přístup

Software je jen tak bezpečný, jak bezpečný je jeho nejslabší článek. Investujeme své odborné znalosti a finanční prostředky do zvýšení bezpečnosti celého ekosystému open source. Náš tým vývojářů a bezpečnostních expertů věří, že dokážeme ochránit více veřejných i soukromých organizací následujícími způsoby:

Náš tým kontroluje každou fázi životního cyklu produktu, průběžně skenuje, analyzuje a fuzz testuje na zranitelnosti.

Podporujeme otevřený internet, sdílíme své poznatky s komunitou vývojářů a zajišťujeme jeho bezpečnost pro veřejnost a podniky.

Zvyšujeme bezpečnost do budoucna tím, že detekujeme sofistikované hrozby, poskytujeme pokročilé automatizované nástroje a jsme o krok napřed před tím, co přijde.

Zabezpečení softwaru s otevřeným zdrojovým kódem je společná odpovědnost a my jsme odhodláni pokračovat ve spolupráci na tomto naléhavém a zásadním problému. g.co/security/gosst

Zdroje: 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. Sdílení našich znalostí (tj. vydání SLSA, vedení OpenSSF) znamená, že všichni, kdo vytvářejí software, nejen Google, mohou těžit ze zkušeností a časem ověřených bezpečnostních postupů společnosti Google. 5. SLSA je soubor postupů, které pomohou organizacím zlepšit bezpečnost jejich procesu vývoje softwaru. Pomáhá splnit požadavky rámce vlády USA pro bezpečný vývoj softwaru, stanovené v reakci na exekutivní nařízení o kybernetické bezpečnosti. To znamená, že organizace budou mít k dispozici rady, jak dodržovat federální pokyny, aby byl software bezpečnější pro všechny.