Захист основи для розробки програмного забезпечення

З різким зростанням кількості кібератак і зловмисників в Інтернеті ми вважаємо, що наші продукти й послуги корисні настільки, наскільки вони безпечні. У Google ми як ніколи зосереджені на захисті людей, організацій і урядів. Ми ділимося нашим досвідом, розширюємо можливості суспільства протистояти кіберризикам, що постійно зростають, і працюємо над тим, щоб підняти сучасний рівень кібербезпеки й зробити світ безпечнішим для всіх.

Програмне забезпечення з відкритим вихідним кодом – тобто з кодом, який надається у вільний доступ, щоб будь-хто міг його використовувати, модифікувати й розбудовувати – є основою сучасного Інтернету. Світ розробки програмного забезпечення з відкритим кодом дозволяє співпрацювати й швидко впроваджувати інновації шляхом вільного обміну рішеннями. Проте сама відкритість, яка робить цифровий світ доступним для всіх, також робить його винятково вразливим до загроз безпеці.

Виклик

Програмне забезпечення з відкритим кодом хвилює кожного

Спільнота розробників додатків із відкритим кодом, в основі якої лежать принципи прозорості й спільного використання, додає величезну кількість коду до більшості додатків, які ми використовуємо сьогодні. Від медичного обладнання до електромережі, люди покладаються на програмне забезпечення з відкритим кодом практично щодня і щогодини, що робить проекти з відкритим кодом основною мішенню для кібератак. Останні три роки ми бачимо, що кількість атак на ланцюжки постачання програмного забезпечення зросла до 742% за рік[1].

Екосистема відкритого вихідного коду є складною і багаторівневою, де приховані непрямі залежності можуть містити недоліки безпеки. Завдяки цим рівням важко виявити вразливості вручну, тому захист цієї частини розробки програмного забезпечення став актуальною проблемою безпеки в усьому світі.

Потрібна додаткова увага на всіх рівнях:

- Розробникам програмного забезпечення з відкритим кодом потрібні знання і ресурси, щоб захистити свої проекти
- Організаціям необхідно розуміти ризики й вразливі місця ланцюжка постачання, щоб розробити плани реагування і мінімізації ризиків
- Уряди й галузь загалом повинні співпрацювати, щоб забезпечити надійні ефективні стандарти безпеки[3]

ВІДСОТОК ГАЛУЗЕВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ЩО МІСТИТЬ ВІДКРИТИЙ КОД[2]

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

Наше рішення

Захист програмного забезпечення з відкритим кодом для всіх

У Google ми працюємо над цим завданням роками. Насправді кожен рік більше ніж 10% користувачів Google роблять внесок у проекти програмного забезпечення з відкритим кодом. Наш досвід приводить нас до висновку, що сучасна цифрова безпека насправді може бути реалізована за рахунок прийняття відкритого підходу. Відкритий код дає нам змогу швидше впроваджувати останні інновації, а також допомагає більшій кількості людей вирішувати проблеми безпеки. Але щоб повністю розкрити цінність відкритого коду, нам потрібні міцніші державно-приватні партнерства й динамічні схеми правил для зміцнення безпеки для всіх. Ось чому ми вітаємо зусилля уряду США щодо покращення безпеки ПЗ з відкритим кодом, як-от закон "Про безпеку програмного забезпечення з відкритим кодом", представлений Сенатом у 2022 році.

- Ми очолюємо спільноту, створюючи такі інфраструктури безпеки наступного покоління, як Supply-chain Levels for Software Artifacts (SLSA),[4,5] і розробляючи передові інструменти безпеки.
- Ми започаткували ініціативу Graph for Understanding Artifact Composition (GUAC), що об'єднує інформацію про безпеку програмного забезпечення з різних джерел у єдину базу даних із можливістю запиту даних. GUAC буде демократизувати доступність інформації про безпеку, роблячи її вільно доступною і корисною для кожної організації.

Наші зобов'язання:

- Інвестувати 100 мільйонів доларів у безпеку додатків з відкритим кодом, керівні посади в Open Source Security Foundation і пряму співпрацю з розробниками
- Визначити та поширити дієві стандарти безпеки, інструкції, безкоштовні інструменти та найкращі методи , які ми використовуємо внутрішньо, в усій спільноті з відкритим кодом
- Покращити виявлення, автоматизоване сортування і способи створення інструментів захисту на ранніх стадіях розробки
- Автоматизувати використання інструментів, щоб зробити безпеку корпоративного рівня безкоштовною та доступною для всіх

Додатки

Google OSS Fuzz
Наша відповідь на помилку Heartbleed

Помилка Heartbleed була серйозною вразливістю відкритого вихідного коду, слабкою стороною, яка могла вплинути майже на кожного користувача Інтернету. У 2014 році хакери викрали імена, адреси, дати народження, номери телефонів і номери соціального страхування приблизно 4,5 млн пацієнтів з бази даних однієї з найбільших лікарень США

У відповідь компанія Google запустила OSS-Fuzz як безкоштовний сервіс для спільноти. Тестування Fuzz виявляє невідомі недоліки безпеки за лічені хвилини, на відміну від ручного тестування, яке може тривати місяцями. Ми інвестували у створення інфраструктури для автоматичного тестування сотень проектів із відкритим кодом. Тепер OSS-Fuzz регулярно сканує код і постійно впроваджує інновації, щоб виявляти більше класів помилок.

Відсканована понад 800 критичних проектів з відкритим кодом з використанням тестування Fuzz шістьма мовами.

Наші галузеві інвестиції та віхи

2020 — СЕРПЕНЬ
Приєднання до форуму Open Source Security Foundation (OpenSSF) для підвищення безпеки програмного забезпечення з відкритим кодом

2021 — ТРАВЕНЬ І ЧЕРВЕНЬ
Встановлено найкращі методи застосування OSS відповідно до **Виконавчого наказу Білого дому 14028** і надано рекомендації щодо стандартів безпеки ланцюжка постачання програмного забезпечення.

ЧЕРВЕНЬ
Випущено SLSA з OpenSSF, що виводить назовні інфраструктуру внутрішньої безпеки Google і дозволяє кожному створювати більш безпечне програмне забезпечення.

СЕРПЕНЬ
Виділено 100 мільйонів доларів США на вдосконалення і захист OSS, включно зі співпрацею з розробниками для пошуку й усунення вразливостей

2022 — ТРАВЕНЬ
Під час Саміту DC було **оголошено про групу підтримки відкритого вихідного коду Google,** яка виділила команду штатних розробників для безпосередньої роботи з проектами з відкритим кодом для покращення їх безпеки.

ТРАВЕНЬ
Анонсовано програмний продукт Assured Open Source, який допомагає інтегрувати ті самі надійні пакети ПЗ з відкритим кодом, які використовує Google, у робочі процеси розробників.

Методи, рекомендовані Google, які можуть допомогти державним і приватним організаціям залишатися в безпеці сьогодні:

- Запровадження SLSA для посилення безпеки ланцюжка постачання програмного забезпечення
- Криптографічні підписи і перевірка автентичності вашого програмного забезпечення за допомогою Sigstore
- Автоматизація виявлення вразливостей, відстеження та сортування за допомогою OSS-Fuzz і OSV.dev
- Використання Scorecards для автоматичної оцінки ризику безпеки з вашими залежностями

Наш підхід

Програмне забезпечення безпечне настільки, наскільки безпечна його найслабша ланка. Ми інвестуємо наш досвід і фінансові ресурси для підвищення безпеки всієї екосистеми відкритого коду. Наші спеціалісти з розробки й безпеки вважають, що ми можемо захистити більше державних і приватних організацій такими способами:

Наша команда перевіряє кожну стадію життєвого циклу продукту, безперервно скануючи, аналізуючи й перевіряючи її на вразливості

Ми підтримуємо відкритий Інтернет, ділимося своїми знаннями зі спільнотою розробників і забезпечуємо захист для громадськості й компаній

Ми забезпечуємо захист на майбутнє, виявляючи складні загрози, надаючи розширені автоматизовані інструменти й залишаючись на крок попереду будь-яких подій

Захист програмного забезпечення з відкритим вихідним кодом є спільною відповідальністю, і ми будемо продовжувати співпрацювати над цією критично важливою проблемою з іншими компаніями. g.co/security/gosst

Джерела: 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. Коли ми говоримо про те, що ділимося своїми знаннями й досвідом (як-от випуск SLSA, очолення OpenSSF), це означає, що кожен, хто створює програмне забезпечення, а не лише компанія Google, може скористатися досвідом Google і перевіреними часом методами підвищення безпеки. 5. SLSA – це набір методів, які можуть допомогти організаціям підвищити безпеку процесу розробки програмного забезпечення. Вони допомагають виконувати вимоги уряду США про безпечну розробку програмного забезпечення (Secure Software Development Framework), викладені у відповідь на виконавчий наказ про кібербезпеку. Це означає, що організації матимуть вказівки щодо того, як дотримуватися федеральних інструкцій, щоб зробити програмне забезпечення більш безпечним для всіх.