Bezpieczne podstawy tworzenia oprogramowania

W obliczu drastycznego nasilenia się cyberataków sponsorowanych przez władze państwowe i przestępczości internetowej jesteśmy przekonani, że nasze produkty i usługi mogą być przydatne tylko wtedy, gdy będą bezpieczne. Google jeszcze bardziej niż dotychczas skupia się na ochronie ludzi, organizacji i władz państwowych. Dzielimy się swoją specjalistyczną wiedzą, motywujemy społeczeństwo do reagowania na nieustannie zmieniające się czynniki ryzyka w cyberprzestrzeni i stale pracujemy nad poprawą stanu wiedzy w zakresie cyberbezpieczeństwa, by uczynić świat bezpieczniejszym dla wszystkich.

Oprogramowanie open source – czyli kod, który jest publicznie dostępny i który każdy może wykorzystywać, modyfikować i rozwijać – stanowi podstawę współczesnego internetu. Programowanie open source umożliwia współpracę i dynamiczne wprowadzanie innowacji dzięki udostępnianiu opracowanych rozwiązań bezpłatnie. Jednak ta otwartość, dzięki której cyfrowy świat jest dostępny dla każdego, stanowi o jego wyjątkowej podatności na zagrożenia.

Wyzwanie

Oprogramowanie open source to nasze wspólne wyzwanie

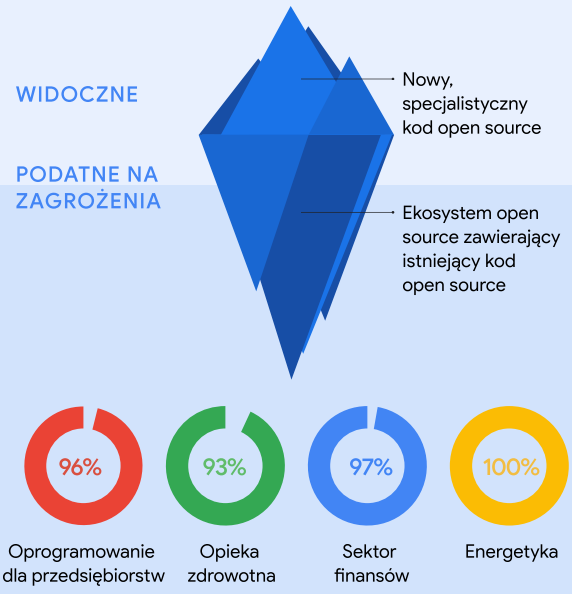
Społeczność zajmująca się tworzeniem oprogramowania open source, oparta na zasadach przejrzystości i dzielenia się, jest źródłem ogromnych ilości kodu do większości używanych obecnie aplikacji. Ludzie polegają na oprogramowaniu open source praktycznie przez okrągłą dobę. Znajdziemy je zarówno w urządzeniach medycznych, jak i w sieci energetycznej. To sprawia, że projekty open source są doskonałym celem cyberataków. Przez trzy ostatnie lata liczba ataków na łańcuch dostaw oprogramowania rosła o 742% rok do roku[1].

Ekosystem open source jest skomplikowany i wielowarstwowy, a ukryte w nim pośrednie zależności mogą zawierać luki w zabezpieczeniach. Wielowarstwowość utrudnia ręczne wykrywanie luk, dlatego zabezpieczenie tego elementu tworzenia oprogramowania stało się poważnym problemem na całym świecie.

To zagadnienie wymaga więcej uwagi na wszystkich szczeblach:

- Twórcy oprogramowania open source potrzebują wiedzy i zasobów, żeby móc zabezpieczać swoje projekty
- Organizacje muszą posiadać wiedzę o zagrożeniach i lukach w łańcuchu dostaw, żeby opracowywać plany przeciwdziałania zagrożeniom
- Władze państwowe i branża oprogramowania muszą współpracować ze sobą, żeby wprowadzić solidne i skuteczne standardy bezpieczeństwa[3]

PROCENTOWY UDZIAŁ OPROGRAMOWANIA DLA DANEJ BRANŻY ZAWIERAJĄCEGO KOD OPEN SOURCE[2]



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

Nasze rozwiązanie

Zabezpieczamy oprogramowanie open source dla wszystkich

Google pracuje nad tym wyzwaniem od lat. Co roku 10% pracowników Google uczestniczy w projektach związanych z oprogramowaniem open source. Z naszego doświadczenia wynika, że aby zadbać o bezpieczeństwo cyfrowe w nowoczesny sposób, trzeba wykorzystać tę otwartość. Dzięki otwartości możemy szybko wprowadzać najnowsze innowacje, a rozwiązywaniem problemów bezpieczeństwa zajmuje się więcej osób. Aby jednak móc w pełni wykorzystać zalety koncepcji open source, potrzebne są silniejsze partnerstwa publiczno-prywatne i dynamiczne ramy polityczne, które zapewnią bezpieczeństwo wszystkim. Dlatego bardzo nas cieszą działania na rzecz bezpieczeństwa oprogramowania open source podejmowane przez rząd amerykański, takie jak ustawa o zabezpieczaniu oprogramowania open source (Securing Open Source Software Act), przedstawiona w Senacie w 2022 r.

- Podejmujemy pionierskie działania w skali całej branży, wprowadzając udoskonalone ramy bezpieczeństwa, takie jak Supply-chain Levels for Software Artifacts (SLSA)[4,5], oraz opracowując zaawansowane narzędzia zabezpieczeń.
- Opracowaliśmy Graph for Understanding Artifact Composition (GUAC), który gromadzi informacje o bezpieczeństwie oprogramowania pochodzące z różnych źródeł w jednej bazie danych z możliwością odpytywania. GUAC demokratyzuje dostęp do informacji dotyczących bezpieczeństwa, ponieważ bezpłatnie udostępnia przydatne informacje każdej organizacji.

Nasze zobowiązania:

- Zainwestujemy 100 mln dolarów w bezpieczeństwo open source, stanowiska kierownicze w Open Source Security Foundation oraz bezpośrednią współpracę z twórcami oprogramowania
- Określimy i będziemy udostępniać całej społeczności open source praktyczne standardy bezpieczeństwa, wytyczne, bezpłatne narzędzia i najlepsze praktyki, które stosujemy w firmie
- Udoskonalimy wykrywanie zagrożeń, automatyczne nadawanie priorytetów oraz metody uwzględnienia bezpieczeństwa już na najwcześniejszych etapach rozwoju oprogramowania
- Zautomatyzujemy narzędzia, aby zabezpieczenia klasy enterprise były bezpłatne i dostępne dla wszystkich

Google OSS Fuzz
Nasza odpowiedź na błąd Heartbleed

Błąd Heartbleed był poważną luką bezpieczeństwa w oprogramowaniu open source, która stanowiła zagrożenie dla prawie wszystkich internautów. W 2014 r. hakerzy wykradli imiona i nazwiska, adresy, daty urodzenia, numery telefonów i numery ubezpieczenia społecznego ok. 4,5 mln pacjentów z bazy danych jednego z największych amerykańskich szpitali.

W odpowiedzi firma Google uruchomiła OSS-Fuzz, darmową usługę dla społeczności. Fuzz testing wskazuje nieznane słabości zabezpieczeń w ciągu paru minut, podczas gdy testowanie ręczne może zająć parę miesięcy. Zainwestowaliśmy w budowę infrastruktury do automatycznego testowania setek projektów open source. Obecnie OSS-Fuzz jest wykorzystywany do regularnego skanowania kodu. Nieustannie wprowadza się do niego innowacje, żeby mógł wykrywać nowe klasy błędów.

Ponad 800 krytycznych projektów open source jest skanowanych metodą Fuzz testing w sześciu językach.

Inwestycje naszej branży i kamienie milowe

2020 — SIERPIEŃ
Dołączyliśmy do Open Source Security Foundation (OpenSSF), by móc kształtować i doskonalić bezpieczeństwo oprogramowania open source.

2021 — MAJ I CZERWIEC
Wprowadziliśmy najlepsze praktyki z obszaru oprogramowania open source zgodnie z rozporządzeniem wykonawczym Prezydenta Stanów Zjednoczonych nr 14028 i udostępniliśmy wytyczne w zakresie standardów bezpieczeństwa w łańcuchu dostaw oprogramowania.

CZERWIEC
Opublikowaliśmy SLSA i OpenSSF. W ten sposób udostępniamy wewnętrzne ramy bezpieczeństwa Google oraz umożliwiamy każdemu tworzenie bezpieczniejszego oprogramowania.

SIERPIEŃ
Przeznaczyliśmy 100 mln dolarów na poprawę i zabezpieczenie oprogramowania open source, między innymi na partnerską współpracę z twórcami oprogramowania mającą na celu znajdowanie i naprawianie luk zabezpieczeń.

2022 — MAJ
Podczas **szczytu w Waszyngtonie ogłosiliśmy powołanie Open Source Maintenance Crew,** czyli zespołu etatowych programistów, którzy będą pracowali bezpośrednio z projektami open source, aby zwiększyć ich bezpieczeństwo.

MAJ
Ogłaszamy produkt Assured Open Source Software, który umożliwia programistom wykorzystywanie tych samych zaufanych pakietów open source, z których korzysta Google.

Praktyki zalecane przez Google, które pomogą organizacjom publicznym i prywatnym na co dzień dbać o bezpieczeństwo:

- Wdrożyć SLSA w celu utwardzenia bezpieczeństwa łańcucha dostaw
- Stosować podpisy kryptograficzne i sprawdzać autentyczność oprogramowania przy użyciu Sigstore
- Zautomatyzować wykrywanie, monitorowanie i ustalanie priorytetów luk zabezpieczeń, korzystając z OSS-Fuzz i OSV.dev
- Używać kart wyników (Scorecards) do automatycznej oceny ryzyka bezpieczeństwa w ramach swoich zależności

Nasze podejście

Oprogramowanie jest tak bezpieczne, jak jego najsłabsze ogniwo. Inwestujemy swoją specjalistyczną wiedzę i środki finansowe w zwiększanie bezpieczeństwa całego ekosystemu open source. Nasz zespół ekspertów od programowania i bezpieczeństwa jest zdania, że dzięki opisanym poniżej działaniom jesteśmy w stanie chronić więcej organizacji publicznych i prywatnych:

Nasz zespół przeprowadza kontrole każdego etapu cyklu życia produktu – nieustannie skanuje, analizuje i przeprowadza fuzz testing pod kątem luk zabezpieczeń

Wspieramy otwarty internet, dzieląc się swoją wiedzą ze społecznością programistów i dbając o bezpieczeństwo internetu dla ogółu społeczeństwa i przedsiębiorstw

Przygotowujemy się na przyszłe wyzwania w obszarze bezpieczeństwa, dostarczając nowoczesne, zautomatyzowane narzędzia oraz wyprzedzając rozwój wydarzeń

Zabezpieczanie oprogramowania open source to nasza wspólna odpowiedzialność i jesteśmy gotowi do dalszej współpracy nad tym pilnym, krytycznym problemem.
g.co/security/gosst

Źródła: 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. Dzielenie się naszą wiedzą (np. udostępnienie SLSA, współtworzenie OpenSSF) oznacza, że każdy twórca oprogramowania, nie tylko Google, może korzystać z naszego doświadczenia i sprawdzonych praktyk w obszarze bezpieczeństwa. 5. SLSA to zbiór praktyk, które ułatwiają organizacjom zabezpieczanie cyklu życia oprogramowania. Pomaga on spełnić wymogi Secure Software Development Framework, które zostały wprowadzone przez rząd amerykański w odpowiedzi na rozporządzenie wykonawcze w sprawie cyberbezpieczeństwa. Oznacza to, że organizacje otrzymują wskazówki dotyczące przestrzegania tych federalnych wytycznych, dzięki którym oprogramowanie stanie się bezpieczniejsze dla wszystkich.