Proteggere le fondamenta dello sviluppo del software

Con il drammatico aumento degli attacchi informatici sponsorizzati dagli Stati e delle minacce online, crediamo che i nostri prodotti e servizi siano utili solo se sicuri. Noi di Google siamo impegnati più che mai a proteggere le persone, le organizzazioni e i governi condividendo le nostre competenze, mettendo la società nelle condizioni di affrontare i rischi informatici in continua evoluzione e lavorando continuamente per far progredire lo stato dell'arte della sicurezza informatica per costruire un mondo più sicuro per tutti.

I software open source, ovvero i codici resi disponibili liberamente a chiunque per l'uso, la modifica e lo sviluppo, oggi sono le fondamenta di Internet. Il mondo dello sviluppo dei software open source permette collaborazioni e rapide innovazioni grazie alla condivisione libera di soluzioni. Tuttavia, proprio l'apertura che rende il mondo digitale accessibile a chiunque, lo rende anche particolarmente vulnerabile a minacce relative alla sicurezza.

La sfida

I software open source sono un problema per tutti

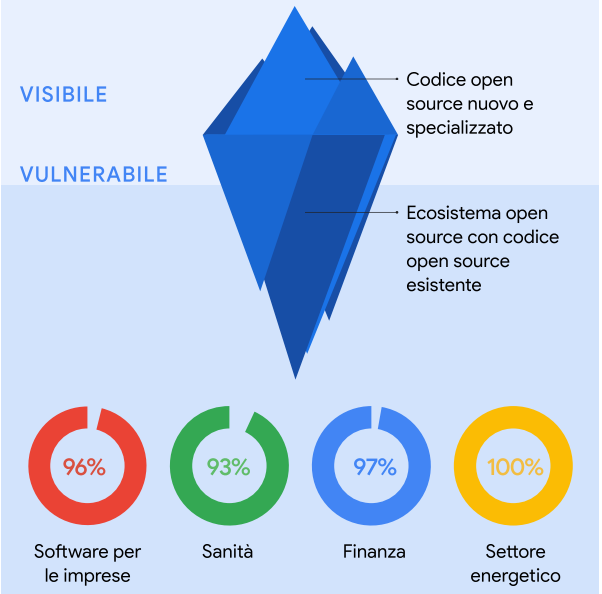
La community degli sviluppatori open source, basata sulla trasparenza e sulla condivisione, contribuisce con un'enorme quantità di codice alla maggior parte delle applicazioni che utilizziamo oggi. Dalle apparecchiature mediche alla rete elettrica, ci si affida ai software open source (OSS) praticamente a ogni ora del giorno, ed è per questo che i progetti open source sono l'obiettivo numero uno degli attacchi informatici. Negli ultimi tre anni si è registrato progressivamente un aumento del 742%[1] degli attacchi alla catena di fornitura dei software.

L'ecosistema open source è intricato e su più livelli, e le dipendenze indirette nascoste possono contenere falle di sicurezza. Questi livelli rendono le vulnerabilità difficili da individuare manualmente, e mettere al sicuro questa parte di sviluppo dei software è diventato un problema di sicurezza urgente a livello globale.

È necessaria una maggiore attenzione a tutti i livelli:

- Gli sviluppatori open source hanno bisogno di conoscenze e risorse per mettere in sicurezza i loro progetti
- Le organizzazioni devono comprendere i rischi e le vulnerabilità della catena di fornitura per sviluppare strategie di mitigazione
- I governi e il settore devono collaborare per assicurare standard di sicurezza resistenti ed efficaci[3]

PERCENTUALE DI SOFTWARE INDUSTRIALI CHE CONTENGONO CODICE OPEN SOURCE[2]



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

La nostra soluzione

Mettere al sicuro i software open source per tutti

Noi di Google lavoriamo da anni a questa sfida. Infatti, ogni anno più del 10% dei Googler contribuisce a progetti di software open source. La nostra esperienza ci porta a concludere che la moderna sicurezza digitale può effettivamente passare da una maggiore apertura. Gli approcci aperti ci assicurano di poter rapidamente adottare le ultime innovazioni e permettere a più persone di risolvere le sfide legate alla sicurezza. Ma per sfruttare appieno il valore dell'open source, abbiamo bisogno di un partenariato pubblico-privato più forte e di quadri strategici più dinamici per rafforzare la sicurezza di tutti. Ecco perché accogliamo con favore l'impegno del governo degli Stati Uniti per promuovere la sicurezza degli OSS, come il Securing Open Source Software Act introdotto al Senato nel 2022.

- Stiamo guidando la comunità con framework di sicurezza di livello superiore, come il Supply-chain Levels for Software Artifacts (SLSA),[4,5] e sviluppando strumenti di sicurezza avanzati.
- Abbiamo sviluppato Graph for Understanding Artifact Composition (GUAC), che raccoglie informazioni sulla sicurezza dei software da diverse fonti in un singolo database interrogabile. GUAC democratizzerà la disponibilità delle informazioni sulla sicurezza rendendole liberamente accessibili e utili per ogni organizzazione.

I nostri impegni:

- Investire 100 milioni di dollari nella sicurezza dell'open source, ricoprire ruoli di leadership nella Open Source Security Foundation e collaborare direttamente con gli sviluppatori
- Definire e condividere standard di sicurezza attuabili, linee guida, strumenti gratuiti e best practice usati internamente con l'intera comunità open source
- Rilevamento avanzato, triage automatizzato e modalità per integrare la sicurezza nelle prime fasi di sviluppo
- Strumenti automatici per rendere la sicurezza a livello aziendale gratuita e accessibile per tutti

Applicazioni

Google OSS Fuzz
La nostra risposta al bug Heartbleed

Il bug Heartbleed è stata una grave vulnerabilità dell'open source, in grado di colpire quasi tutti gli utenti di Internet. Nel 2014 gli hacker rubarono nomi, indirizzi, date di nascita, numeri di telefono e numeri di previdenza sociale di circa 4,5 milioni di pazienti dal database di uno dei maggiori ospedali degli Stati Uniti.

In risposta a ciò, Google ha lanciato OSS-Fuzz come un servizio gratuito per la comunità. Il fuzzing individua vulnerabilità sconosciute in pochi minuti, a differenza dei test manuali che possono richiedere mesi. Abbiamo investito nella realizzazione di un'infrastruttura che testasse automaticamente centinaia di progetti open source. OSS-Fuzz ora esegue regolari scansioni del codice e si innova costantemente per trovare altri tipi di bug.

Più di 800 progetti open source critici vengono analizzati dal fuzzing in sei lingue.

I nostri investimenti e traguardi nel settore

2020 — AGOSTO
Adesione alla Open Source Security Foundation (OpenSSF) per guidare e migliorare la sicurezza dei software open source.

2021 — MAGGIO E GIUGNO
Abbiamo stabilito best practice per gli OSS in conformità con **l'ordine esecutivo 14028 della Casa Bianca** e contribuito a fornire indicazioni sugli standard di sicurezza della catena di fornitura del software.

2021 — GIUGNO
Lancio dell'SLSA con OpenSSF, esternalizzando il framework di sicurezza interno di Google e permettendo a chiunque di costruire software più sicuri.

2021 — AGOSTO
Ci siamo impegnati a stanziare 100 milioni di dollari per migliorare e rendere sicuri gli OSS, anche collaborando con gli sviluppatori per trovare e risolvere le vulnerabilità.

2022 — MAGGIO
Durante un **summit a Washington, Google ha annunciato la sua Open Source Maintenance Crew**, un team di sviluppatori dedicato a tempo pieno direttamente ai progetti open source per migliorarne la sicurezza.

2022 — MAGGIO
Annunciato il prodotto Assured Open Source Software, che consente di incorporare nel flusso di lavoro degli sviluppatori gli stessi pacchetti open source affidabili utilizzati da Google.

Le pratiche raccomandate da Google che possono favorire la sicurezza delle organizzazioni pubbliche e private:

- Implementare l'SLSA per rafforzare la sicurezza della catena di fornitura dei software
- Firmare in maniera crittografica e verificare l'autenticità del software utilizzando Sigstore
- Automatizzare l'individuazione, il monitoraggio e il triage delle vulnerabilità con OSS-Fuzz e OSV.dev
- Usare Scorecards per valutare automaticamente il rischio per la sicurezza delle tue dipendenze

Il nostro approccio

I software sono l'anello debole in fatto di sicurezza. Stiamo investendo le nostre competenze e risorse finanziare per aumentare la sicurezza dell'intero ecosistema open source. Il nostro team di sviluppo e gli esperti di sicurezza sono convinti di poter proteggere più organizzazioni pubbliche e private così:

Il nostro team controlla ogni fase del ciclo di vita del prodotto, effettuando scansioni, analisi e fuzzing continui alla ricerca di vulnerabilità

Sosteniamo l'apertura di Internet, condividendo ciò che sappiamo con la comunità degli sviluppatori e mantenendolo al sicuro per il pubblico e le aziende

Stiamo pensando al futuro della sicurezza, rilevando minacce sofisticate, fornendo strumenti automatizzati avanzati e rimanendo un passo avanti rispetto a ciò che verrà

Rendere sicuri i software open source è una responsabilità condivisa, e ci impegniamo a collaborare per risolvere questo problema urgente e grave. g.co/security/gosst

Fonti: 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. Condividere informazioni (ad esempio, distribuendo l'SLSA, guidando l'OpenSSF) significa che tutti coloro che producono software, non solo Google, possono beneficiare dell'esperienza e delle pratiche di sicurezza collaudate di Google. 5. SLSA è un insieme di pratiche che possono aiutare le organizzazioni a migliorare la sicurezza del processo di sviluppo dei software. Contribuisce a soddisfare il Secure Software Development Framework del governo degli Stati Uniti, ovvero i requisiti stabiliti dal governo in risposta all'Executive Order sulla cybersicurezza. Ciò significa che le organizzazioni avranno a disposizione una guida su come rispettare le linee guida federali per rendere i software più sicuri per tutti.