Mengamankan fondasi untuk pengembangan perangkat lunak

Peningkatan signifikan serangan siber yang disponsori negara dan pelaku kejahatan di dunia maya membuat kami percaya bahwa produk dan layanan kami hanya akan berguna jika aman. Di Google, kami semakin memfokuskan tujuan kami untuk melindungi masyarakat, organisasi, dan pemerintah dengan membagikan keahlian kami, memberdayakan masyarakat untuk mengatasi risiko siber yang terus berkembang, dan terus berupaya memajukan kecanggihan dalam keamanan siber untuk membangun dunia yang lebih aman bagi semua orang.

Perangkat lunak sumber terbuka — kode yang tersedia secara bebas bagi siapa saja untuk digunakan, dimodifikasi, dan dikembangkan — adalah fondasi internet modern. Dunia pengembangan perangkat lunak sumber terbuka memungkinkan kolaborasi dan inovasi yang cepat dengan berbagi solusi secara bebas. Namun, keterbukaan yang membuat dunia digital dapat diakses oleh semua orang, juga membuatnya rentan terhadap ancaman keamanan.

Tantangan

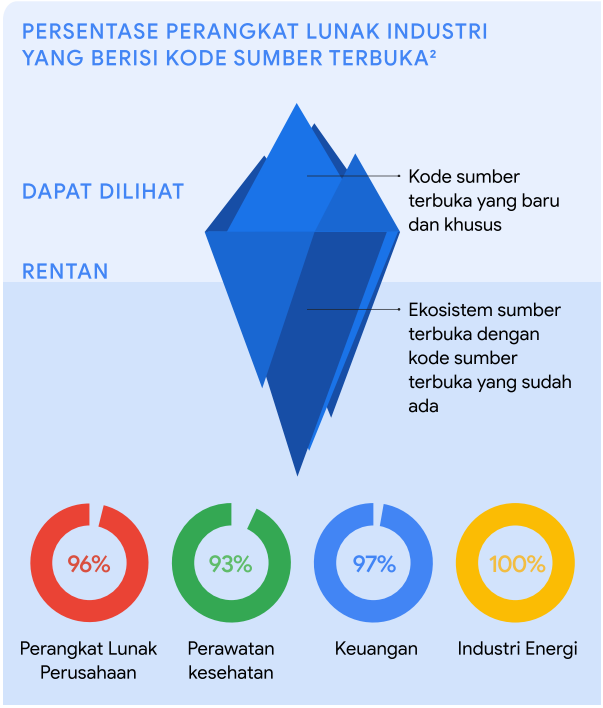
Perangkat Lunak Sumber Terbuka menjadi kekhawatiran semua orang

Komunitas pengembangan sumber terbuka, yang dibangun berdasarkan transparansi dan berbagi, menyumbangkan sejumlah besar kode untuk sebagian besar aplikasi yang kita gunakan saat ini. Dari peralatan medis hingga jaringan listrik, orang-orang mengandalkan perangkat lunak sumber terbuka (open source software/OSS) hampir setiap jam setiap hari—sehingga proyek sumber terbuka menjadi target utama serangan siber. Dalam tiga tahun terakhir, terjadi peningkatan sebesar 742% dari tahun ke tahun[1] dalam serangan rantai pasokan perangkat lunak.

Ekosistem sumber terbuka memiliki banyak lapisan, di mana ketergantungan tidak langsung yang tersembunyi dapat menimbulkan kelemahan keamanan. Lapisan-lapisan ini membuat kerentanan sulit dideteksi secara manual, dan mengamankan bagian pengembangan perangkat lunak ini telah menjadi masalah keamanan yang mendesak secara global.

Fokus tambahan diperlukan di semua tingkatan:

- Pengembang sumber terbuka membutuhkan pengetahuan dan sumber daya untuk mengamankan proyek mereka
- Organisasi perlu memahami risiko dan kerentanan rantai pasokan untuk mengembangkan rencana mitigasi
- Pemerintah dan industri harus bermitra untuk memastikan standar keamanan yang kuat dan efektif[3]



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

Solusi Kami

Mengamankan Perangkat Lunak Sumber Terbuka untuk semua orang

Di Google, kami telah berusaha mengatasi tantangan ini selama bertahun-tahun. Faktanya, setiap tahun lebih dari 10% Pengguna Google berkontribusi di proyek perangkat lunak sumber terbuka. Pengalaman kami menunjukkan bahwa keamanan digital modern sebenarnya dapat dicapai dengan merangkul keterbukaan Pendekatan terbuka memastikan kami dapat dengan cepat mengadopsi inovasi terbaru dan memungkinkan lebih banyak orang untuk menyelesaikan tantangan keamanan. Namun, untuk membuka nilai sumber terbuka sepenuhnya, kita membutuhkan kemitraan publik-swasta yang lebih kuat dan kerangka kerja kebijakan yang dinamis untuk menopang keamanan bagi semua orang. Itulah sebabnya kami menyambut baik upaya Pemerintah AS untuk memajukan keamanan OSS, seperti Undang-Undang Pengamanan Perangkat Lunak Sumber Terbuka yang diperkenalkan di Senat pada tahun 2022.

- Kami memimpin komunitas dengan kerangka kerja keamanan yang canggih, seperti Supply-chain Levels for Software Artifacts (SLSA),[4,5] serta mengembangkan alat keamanan lanjutan.
- Kami telah mengembangkan Graph for Understanding Artifact Composition (GUAC), yang menyatukan informasi keamanan perangkat lunak dari berbagai sumber ke dalam satu basis data yang dapat dikueri. GUAC akan mendemokratisasi ketersediaan informasi keamanan dengan membuatnya dapat diakses secara bebas dan berguna bagi setiap organisasi.

Komitmen Kami:

- Menginvestasikan $100 juta dalam keamanan sumber terbuka, mengemban peran kepemimpinan di Yayasan Keamanan Sumber Terbuka (Open Source Security Foundation), dan melakukan kolaborasi langsung dengan para pengembang
- Menentukan dan membagikan standar keamanan, panduan, alat gratis dan praktik terbaik yang kami gunakan secara internal dan dapat ditindaklanjuti, dengan seluruh komunitas sumber terbuka
- Memajukan deteksi, triase otomatis, dan cara-cara untuk membangun keamanan ke dalam tahap pengembangan paling awal
- Mengotomatiskan alat agar keamanan tingkat perusahaan menjadi gratis dan dapat diakses oleh semua orang

Aplikasi

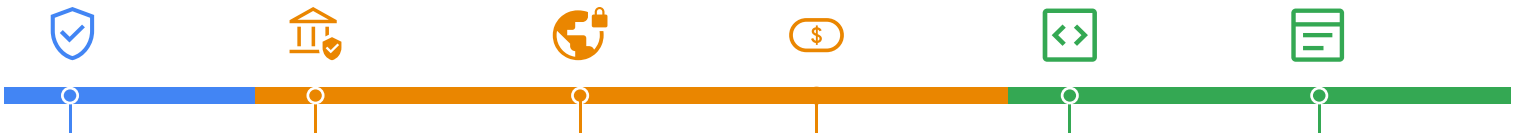
Google OSS Fuzz
Tanggapan kami terhadap bug Heartbleed

Heartbleed bug adalah kerentanan sumber terbuka yang serius, sebuah kelemahan yang berpotensi memengaruhi hampir semua pengguna internet. Pada tahun 2014, para peretas mencuri nama, alamat, tanggal lahir, nomor telepon, dan nomor jaminan sosial dari ~ 4,5 juta pasien dari basis data salah satu rumah sakit terbesar di Amerika Serikat

Sebagai tanggapan, Google meluncurkan OSS-Fuzz sebagai layanan komunitas gratis. Pengujian Fuzz menunjukkan dengan tepat kelemahan keamanan yang tidak diketahui dalam hitungan menit, tidak seperti pengujian manual, yang bisa memakan waktu berbulan-bulan. Kami berinvestasi dalam membangun infrastruktur untuk menguji ratusan proyek sumber terbuka secara otomatis. OSS-Fuzz sekarang menjalankan pemindaian kode secara teratur dan terus berinovasi untuk menemukan lebih banyak kelas bug.

800+ proyek sumber terbuka yang penting dipindai oleh pengujian Fuzz dalam enam bahasa.

Investasi dan Pencapaian Industri Kami



2020 — AGUSTUS
Bergabung dengan Open Source Security Foundation (OpenSSF) untuk memandu dan meningkatkan keamanan perangkat lunak sumber terbuka

2021 — MEI & JUNI
Menetapkan praktik terbaik OSS sesuai dengan **Perintah Eksekutif Gedung Putih 14028** dan menyumbangkan panduan terkait standar keamanan rantai pasokan perangkat lunak.

JUNI
Merilis SLSA dengan OpenSSF, mengeksternalisasi kerangka kerja keamanan internal Google dan memungkinkan semua orang membangun perangkat lunak yang lebih aman.

AGUSTUS
Menjanjikan $100 juta untuk meningkatkan dan mengamankan OSS, termasuk bermitra dengan para pengembang untuk menemukan dan memperbaiki kerentanan

2022 — MEI
Mengumumkan Kru Pemeliharaan Sumber Terbuka Google selama **DC Summit,** mengkhususkan tim pengembang penuh waktu untuk bekerja secara langsung dengan proyek-proyek sumber terbuka guna meningkatkan keamanannya.

MEI
Mengumumkan produk Assured Open Source Software, yang membantu menggabungkan paket sumber terbuka tepercaya yang sama dengan yang digunakan Google ke dalam alur kerja pengembang.

Google merekomendasikan praktik-praktik yang dapat membantu organisasi publik dan swasta tetap aman saat ini:

- Menerapkan SLSA untuk memperkuat keamanan rantai pasokan perangkat lunak
- Menandatangani dan memverifikasi keaslian perangkat lunak Anda secara kriptografis menggunakan Sigstore
- Mengotomatiskan penemuan, pelacakan, dan triase kerentanan dengan OSS-Fuzz dan OSV.dev
- Menggunakan Kartu Skor untuk secara otomatis mengevaluasi risiko keamanan dengan ketergantungan Anda

Pendekatan Kami

Perangkat lunak hanya seaman tautan terlemah. Kami menginvestasikan keahlian dan sumber daya keuangan kami untuk meningkatkan keamanan seluruh ekosistem sumber terbuka. Tim ahli pengembangan dan keamanan kami percaya bahwa kami dapat melindungi lebih banyak organisasi publik dan swasta dengan cara-cara berikut ini:

Tim kami mengaudit setiap tahap siklus hidup produk, memindai, menganalisis, dan menguji secara terus menerus untuk menemukan kerentanan

Kami mendukung internet terbuka, membagikan apa yang kami ketahui kepada komunitas pengembang dan menjaganya tetap aman untuk publik dan bisnis

Kami menyediakan keamanan masa depan dengan mendeteksi ancaman berat, menyediakan alat otomasi yang canggih, dan selalu selangkah lebih maju dari apa pun yang akan terjadi di masa depan

Mengamankan perangkat lunak sumber terbuka merupakan tanggung jawab bersama, dan kami berkomitmen untuk terus berkolaborasi dalam masalah yang sangat penting dan mendesak ini. g.co/security/gosst

Sumber: 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. Dengan membagikan pengetahuan kami (misalnya, merilis SLSA, memandu OpenSSF), semua orang yang membuat perangkat lunak, bukan hanya Google, dapat memperoleh manfaat dari pengalaman dan praktik keamanan Google yang telah teruji oleh waktu, 5. SLSA adalah seperangkat praktik yang dapat membantu organisasi meningkatkan keamanan proses pengembangan perangkat lunak mereka. SLSA membantu memenuhi Kerangka Kerja Pengembangan Perangkat Lunak Aman pemerintah Amerika Serikat, persyaratan yang ditetapkan oleh pemerintah sebagai tanggapan terhadap Perintah Eksekutif terkait keamanan siber. Artinya, organisasi akan memiliki panduan tentang cara mematuhi pedoman federal untuk membuat perangkat lunak lebih aman bagi semua orang.