Google

ओपन सोर्स सिक्योरिटी

सॉफ़्टवेयर डेवलपमेंट के लिए आधार सुरक्षित करना

स्टेट-स्पॉन्सर्ड साइबर हमलों और नुकसान पहुंचाने वालों की ऑनलाइन बढ़ोतरी को देखते हुए, हम मानते हैं कि हमारी प्रोडक्ट और सर्विस ही सहायक हैं क्योंकि उन्हें बेहद सिक्योर बनाया गया है. Google में, हम अपनी विशेषज्ञता को दूसरों से शेयर कर रहे हैं और लोग, संगठन और सरकार की सुरक्षा पर पहले से ज़्यादा ध्यान दे रहे हैं. हम कभी भी सामने आने वाले साइबर जोखिमों से निपटने के लिए समाज को सशक्त बना रहे हैं और हर किसी के लिए एक सुरक्षित माहौल tबनाने के लिए साइबर सिक्योरिटी को एडवांस करने पर लगातार काम कर रहे हैं.

ओपन सोर्स सॉफ़्टवेयर - कोड बेरोक टोक कोई भी इस्तेमाल कर सकता है, इसमें बदलाव भी कर सकता है — यह मॉडर्न इंटरनेट की बुनियाद है. ओपन सोर्स सॉफ्टवेयर डेवलपमेंट की दुनिया में खुले तौर पर समाधान शेयर करके कोलैबोरेशन और तेजी से होने वाला इनोवेशन किया जा सकता है. फिर भी वह खुलापन जो डिजिटल दुनिया को सभी की पहुंच में लाता है, वह इसे असुरक्षित भी बना देता है.

चुनौती

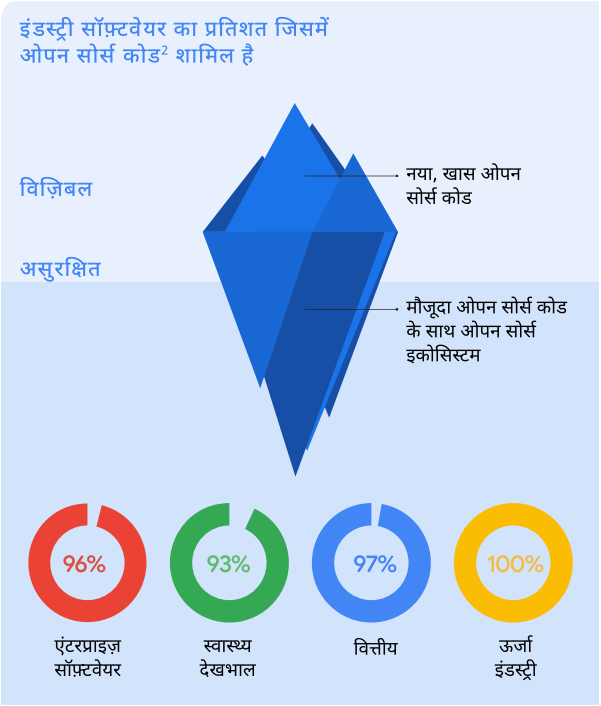
ओपन सोर्स सॉफ़्टवेयर सभी के लिए चिंता का विषय है

ओपन सोर्स डेवलपमेंट कम्युनिटी पारदर्शिता और चीज़ें साझा करने की बुनियाद पर बनी है, वह ऐसे ज़्यादातर ऐप्लिकेशन के कोड में योगदान देती है जिसे आज हम इस्तेमाल करते हैं. मेडिकल इक्विपमेंट से लेकर पावर ग्रिड तक, लोग ओपन सोर्स सॉफ़्टवेयर (OSS) पर वर्चुअली दिन के लगभग हर घंटे भरोसा करते हैं—यही वजह ओपन सोर्स प्रोजेक्ट को साइबर हमलों के लिए एक अहम टारगेट बनाती है. पिछले तीन सालों में सॉफ़्टवेयर सप्लाई चेन हमलों में 742% की साल-दर-साल बढ़ोतरी[1] देखी गई है.

ओपन सोर्स इकोसिस्टम में परतें जटिल हैं, जहां छिपी अप्रत्यक्ष निर्भरता में सिक्योरिटी खामियां हो सकती हैं. ये परतें खामियों की मैन्युअली पहचान करने में कठिनाई लाती है और सॉफ़्टवेयर विकास के इस हिस्से को सुरक्षित करना दुनिया भर में एक ज़रूरी सिक्योरिटी समस्या बन गई है.

हर स्तर पर ज़्यादा ध्यान देने की ज़रूरत है:

- ओपन सोर्स डेवलपर्स को अपने प्रोजेक्ट को सिक्योर करने के लिए नॉलेज और रिसोर्स की ज़रूरत होती है
- गंभीरता घटाने की योजनाओं को बनाने के लिए संगठनों को सप्लाई चेन के जोखिम और कमज़ोरियों को समझने की ज़रूरत है
- मजबूत, असरदार सुरक्षा मानकों के लिए सरकार और इंडस्ट्री को भागीदारी करनी चाहिए



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

हमारा समाधान

सभी के लिए ओपन सोर्स सॉफ़्टवेयर को सुरक्षित करना

Google में, हम सालों से इस चुनौती पर काम कर रहे हैं. वास्तव में, हर साल 10% से ज़्यादा Googlers ओपन सोर्स सॉफ़्टवेयर प्रोजेक्ट में योगदान देते हैं. हमारा अनुभव हमें इस निष्कर्ष पर ले जाता है कि आधुनिक डिजिटल सिक्योरिटी वास्तव में खुलेपन को अपनाने से मिल सकती है. खुला नज़रिया यह निश्चित करता है कि हम नए इनोवेशन को तेज़ी से अपना सकें और ज़्यादा लोगों को सिक्योरिटी चुनौतियों का समाधान करने के लिए तैयार कर सकें. लेकिन ओपन सोर्स की वैल्यू को पूरी तरह इस्तेमाल करने के लिए, हमें सभी के लिए सिक्योरिटी को बेहतर बनाने के लिए मज़बूत सार्वजनिक-निजी भागीदारी और असरदार नीतिगत ढांचे की ज़रूरत है. इसलिए हम OSS सिक्योरिटी को आगे बढ़ाने के अमेरिकी सरकार की कोशिशों का स्वागत करते हैं, जैसे Securing Open Source Software Act. इसे 2022 में सीनेट में पेश किया गया था.

- हम अगले लेवल के सिक्योरिटी ढांचे के साथ कम्युनिटी का नेतृत्व कर रहे हैं, जैसे Supply-chain Levels for Software Artifacts (SLSA),[4,5] और एडवांस सिक्योरिटी टूल डेवलप करना.
- हमने Graph for Understanding Artifact Composition (GUAC) को डेवलप किया है. यह कई सोर्स से सॉफ़्टवेयर सिक्योरिटी जानकारी को एक क्वेरी के डेटाबेस में साथ लाता है. GUAC इसे हर संगठन के लिए खुले तौर पर एक्सेस करने लायक और काम का बनाकर सिक्योरिटी जानकारी की उपलब्धता को आसान बनाएगा.

हमारी प्रतिबद्धताएं:

- ओपन सोर्स सिक्योरिटी में $100 मिलियन का निवेश, Open Source Security Foundation में नेतृत्व भूमिका और डेवलपर्स के साथ सीधा कोलैबोरेशन
- **जिन कार्रवाई योग्य सिक्योरिटी स्टैंडर्ड, गाइडैंस,** फ़्री टूल और बेस्ट प्रैक्टिस का इस्तेमाल हम आंतरिक रूप से करते हैं, उन्हें पूरी ओपन सोर्स कम्यूनिटी के साथ डिफ़ाइन करना और शेयर करना
- अडवांस डिटेक्शन, ऑटोमेटेड ट्राइएजिंग और शुरुआती डेवलपमेंट स्टेज में सुरक्षा पुख्ता करने के तरीके
- ऑटोमेटेड टूलिंगएंटरप्राइस -लेवल की सिक्योरिटी को फ़्री और सभी की पहुंच में लाना

ऐप्लिकेशन

Google OSS Fuzz
हार्टब्लीड बग पर हमारी प्रतिक्रिया

हार्टब्लीड बग एक गंभीर ओपन सोर्स खामी थी, ये लगभग हर इंटरनेट यूज़र को प्रभावित करने वाली चूक थी. 2014 में, हैकर्स ने अमेरिका के सबसे बड़े अस्पतालों में से एक के डेटाबेस से ~45 लाख मरीज़ों[b] के नाम, पते, जन्मतिथि, फ़ोन नंबर और सोशल सिक्योरिटी नंबर चुरा लिए थे

इससे निपटने के लिए, Google ने OSS-Fuzz को एक फ़्री कम्युनिटी सर्विस के रूप में लॉन्च किय. मैन्युअल टेस्टिंग से उलट, Fuzz टेस्टिंग छिपी हुई सिक्योरिटी खामी को मिनटों में तलाश सकती है. मैन्युअल टेस्टिंग के ज़रिए इसमें महीने लग सकते हैं. हमने सैकड़ों ओपन सोर्स प्रोजेक्ट को ऑटोमैटिकली टेस्ट करने के लिए इंफ़्रास्ट्रक्चर बनाने में निवेश किया है. OSS-Fuzz अब नियमित रूप से कोड स्कैन करता है और बगों की ज़्यादा क्लास तलाशने के लिए नए बदलाव कर रहा है.

छह भाषाओं में **Fuzz टेस्टिंग से 800+ क्रिटिकल ओपन सोर्स प्रोजेक्ट स्कैन किए गए.**

हमारा इंडस्ट्री निवेश और मुकाम

2020

अगस्त
ओपन सोर्स सॉफ़्टवेयर की सिक्योरिटी को गाइड करने और उसमें सुधार के लिए **Open Source Security Foundation (OpenSSF)** जॉइन किया

2021

मई और जून
White House Executive Order 14028 के नियमों के मुताबिक **OSS** बेस्ट प्रैक्टिस की स्थापना की और सॉफ़्टवेयर सप्लाई चेन सिक्योरिटी स्टैंडर्ड के मार्गदर्शन में योगदान दिया.

जून
OpenSSF के साथ SLSA जारी किया, Google के आंतरिक सिक्योरिटी ढांचे को अमल में लाया और सभी को ज़्यादा सिक्योर सॉफ़्टवेयर बनाने के लिए प्रेरित किया.

अगस्त
कमजोरियों को खोजने और ठीक करने के लिए डेवलपर्स के साथ साझेदारी सहित **OSS को बढ़ाने और सिक्योर करने के लिए $100M का वादा किया**

2022

मई
DC Summit के दौरान Google के Open Source Maintenance Crew की घोषणा की, सिक्योरिटी में सुधार के लिए फुल-टाइम डेवलपर्स की टीम को सीधा ओपन सोर्स प्रोजेक्ट पर काम करने के लिए नियुक्त किया.

मई
Assured Open Source Software प्रोडक्ट की घोषणा की, जो उन्हीं विश्वसनीय ओपन सोर्स पैकेजों को शामिल करने में मदद करता है जिनका इस्तेमाल Google डेवलपर वर्कफ़्लो में करता है.

Google द्वारा सुझाए गए तरीके जो आज सरकारी और निजी संगठनों को सुरक्षित रखने में मदद कर सकते हैं:

- सॉफ़्टवेयर सप्लाई चेन सिक्योरिटी मज़बूत करने के लिए SLSA लागू करें
- Sigstore का इस्तेमाल करके अपने सॉफ़्टवेयर की प्रामाणिकता को क्रिप्टोग्राफ़िक रूप से साइन और वेरिफ़ाई करें
- OSS-Fuzz और OSV.dev के साथ खामियों को तलाशने, उनकी ट्रैकिंग और ट्राइएजिंग को ऑटोमेट करें
- अपनी निर्भरताओं के साथ सिक्योरिटी जोखिम को ऑटोमैटिकली पता लगाने के लिए स्कोरकार्ड का इस्तेमाल करें

हमारा नज़रिया

सॉफ़्टवेयर सिर्फ़ सबसे कमजोर कड़ी जितना ही सिक्योर है. हम पूरे ओपन सोर्स इकोसिस्टम की सिक्योरिटी बढ़ाने के लिए अपनी विशेषज्ञता और वित्तीय संसाधनों को लगा रहे हैं. डेवलपमेंट और सिक्योरिटी एक्सपर्ट की हमारी टीम का मानना है कि हम इन तरीकों से और सरकारी और निजी संगठनों की और भी ज़्यादा सुरक्षा कर सकते हैं:

हमारी टीम कमजोरियों का पता लगाने के लिए प्रोडक्ट की लाइफ़स्टाइल के हर स्टेज, लगातार होने वाली स्कैनिंग, विश्लेषण और फ़ज़ टेस्टिंग की ऑडिट करती है

हम ओपन इंटरनेट को सपोर्ट करते हैं, जानकारी को डेवलपर कम्युनिटी संग बांटते हैं और जनता और कारोबार के लिए इसे सुरक्षित बनाते हैं.

हम जटिल खतरों का पता लगाकर, एडवांस ऑटोमेटेड समाधान देते हैं और आगे जो भी समस्या आती है, उससे एक कदम आगे रहकर सिक्योरिटी को भविष्य के लिए बेहतर बना रहे हैं

ओपन सोर्स सॉफ़्टवेयर को सुरक्षित करना एक साझा ज़िम्मेदारी है और हम इस बेहद ज़रूरी, गंभीर समस्या पर कोलैबोरेशन जारी रखने के लिए प्रतिबद्ध हैं. g.co/security/gosst

Sources: 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. हमारी जानकारी को साझा करने (यानी, SLSA जारी करना, OpenSSF का मार्गदर्शन करना) का मतलब है कि सॉफ़्टवेयर बनाने वाला हर इंसान, सिर्फ़ Google ही नहीं, Google के अनुभव और वक्त-वक्त पर अपनाए गए सुरक्षा के तरीकों से फ़ायदा उठा सकता है, 5. SLSA ऐसे तरीकों का एक समूह है जो संगठनों को उनके सॉफ़्टवेयर डेवलपमेंट प्रोसेस की सिक्योरिटी में सुधार करने में मदद कर सकता है. यह US सरकार के Secure Software Development Framework के मुताबिक काम करने में मदद करता है. ये ज़रूरतें साइबर सिक्योरिटी पर कार्यकारी आदेश के जवाब में सरकार की ओर से तय की गई हैं. इसका मतलब है कि संगठनों के पास मार्गदर्शन होगा कि सॉफ़्टवेयर को सभी के लिए ज़्यादा सिक्योर बनाने के लिए संघीय दिशानिर्देशों का पालन कैसे किया जाए.