Yazılım geliştirmenin temelini koruyoruz

Devlet destekli siber saldırılar ve çevrimiçi kötü amaçlı aktörlerin sayısında görülen önemli artışla birlikte ürün ve hizmetlerimizin faydalı olmalarının yanı sıra güvenli olmaları gerektiğine de inanıyoruz. Google olarak; uzmanlığımızı paylaşarak, sürekli değişen siber riskleri ele almak için toplumu güçlendirerek ve herkes için daha güvenli bir dünya inşa etme amacıyla en son siber güvenlik teknolojisinde ilerleme sağlamak için sürekli çalışarak insanları, kuruluşları ve devletleri korumaya her zamankinden daha çok odaklanıyoruz.

Herkesin kullanabileceği, değiştirebileceği ve üzerine inşa edebileceği kod olan açık kaynak yazılım, modern internetin temelidir. Açık kaynak yazılım geliştirme dünyası, çözümleri ücretsiz olarak paylaşarak iş birliği ve hızlı inovasyon sağlar. Ancak dijital dünyanın herkes için erişilebilir olmasını sağlayan aynı açıklık, aynı zamanda onu güvenlik tehditlerine karşı benzersiz şekilde savunmasız hâle getiriyor.

Zorluk

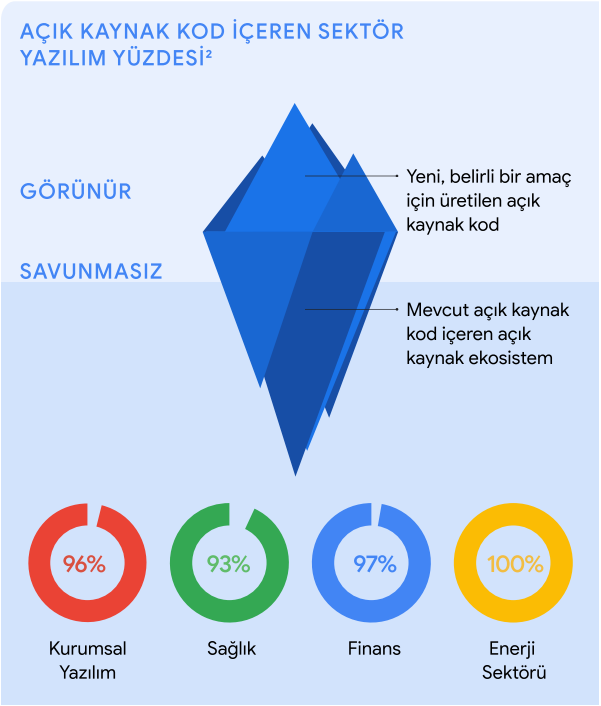
Açık Kaynak Yazılım herkes için bir endişe konusudur

Şeffaflık ve paylaşım üzerine inşa edilmiş olan açık kaynak geliştirme topluluğu, bugün kullandığımız uygulamaların çoğu için muazzam miktarda kod sağlar. Tıbbi ekipmanlardan enerji nakil şebekesine, insanlar günün her saatinde açık kaynak yazılımı (OSS) kullanıyor; bu durum da açık kaynak projelerini siber saldırılar için ana hedef hâline getiriyor. Geçtiğimiz üç yıl içerisinde yazılım tedarik zinciri saldırılarında yıldan yıla %742 artış[1] görüldü.

Açık kaynak ekosistemi, gizli dolaylı bağlılıkların güvenlik zafiyetleri içerebileceği karmaşık bir şekilde katmanlandırılmıştır. Bu katmanlar güvenlik açıklarının manuel olarak saptanmasını zorlaştırır ve yazılım geliştirmenin bu kısmının korunması küresel boyutta acil bir güvenlik sorunu hâline gelmiştir.

Her seviyede ekstra odaklanma gerekli:

- Açık kaynak geliştiricileri projelerini korumak için bilgiye ve kaynaklara ihtiyaç duyar.
- Kuruluşların riskleri azaltma yönünde planlar geliştirmek için tedarik zinciri risklerini ve güvenlik açıklarını anlamaları gerekir.
- Devletler ve sektör, güçlü ve etkili güvenlik standartları sağlamak için birlikte çalışmalıdır[3].



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

Çözümümüz

Açık Kaynak Yazılımı herkes için koruma

Google olarak, yıllardır bu zorluk üzerinde çalışıyoruz. Aslına bakılırsa, her yıl %10'u aşkın Google çalışanı açık kaynak yazılım projelerine katkıda bulunuyor. Deneyimlerimiz sonucunda modern dijital güvenliğin açıklığın benimsenmesiyle sağlanabileceğini düşünüyoruz. Açık yaklaşımlar en son inovasyonları hızla benimsememizi ve daha fazla insanın güvenlik zorluklarını çözmesini sağlıyor. Ancak açık kaynağın değerini tam olarak ortaya çıkarmak için daha güçlü kamu-özel sektör ortaklıklarına ve herkes için güvenliği desteklemek amacıyla dinamik politika çerçevelerine ihtiyacımız var. İşte bu sebeple, 2022 yılında Senato tarafından yürürlüğe konulan Açık Kaynak Kodlu Yazılımın Güvenliğini Sağlama Yasası gibi OSS güvenliğini geliştirmek için ABD Hükûmeti tarafından atılan adımları destekliyoruz.

- Yazılım Eserleri için Tedarik Zinciri Seviyeleri (SLSA),[4,5] gibi bir üst seviye güvenlik çerçeveleri ve ileri güvenlik araçları geliştirerek topluluğa öncülük ediyoruz.
- Farklı kaynaklardan yazılım güvenliği bilgilerini sorgulanabilir tek bir veri tabanında bir araya getiren Eser Kompozisyonunu Anlama Grafiğini (GUAC) geliştirdik. GUAC, güvenlik bilgilerini her kuruluş için serbestçe erişilebilir ve kullanışlı hâle getirerek bu bilgilerin kullanılabilirliğini yaygınlaştıracak.

Taahhütlerimiz:

- Açık Kaynak Güvenlik Vakfı'nda liderlik rolleri ve geliştiriciler ile doğrudan iş birliği için 100 milyon $ yatırımda bulunmak
- Şirket içinde kullandığımız uygulanabilir güvenlik standartlarını, rehberliği, ücretsiz araçları ve en iyi uygulamaları tanımlamak ve tüm açık kaynak topluluğu ile paylaşmak
- Gelişmiş tespit, otomatik önceliklendirme ve güvenliği en erken geliştirme aşamalarına dâhil etmenin yollarını geliştirmek
- Kurumsal seviyede güvenliği herkes için ücretsiz ve erişilebilir yapmak için araçları otomatikleştirmek

Google OSS Fuzz
Heartbleed hatasına yanıtımız

Heartbleed hatası ciddi bir açık kaynak güvenlik açığı ve hemen hemen her internet kullanıcısını etkileme potansiyeline sahip bir zafiyetti. Bilgisayar korsanları, 2014 yılında ABD'nin en büyük hastanelerinden birinin veri tabanından yaklaşık 4,5 milyon hastanın ismini, adresini, doğum tarihini, telefon numarasını ve sosyal güvenlik numarasını çaldı.

Google, buna yanıt olarak ücretsiz bir topluluk hizmeti olarak OSS-Fuzz 'ı hizmete sundu. Fuzz testi, aylar alabilecek manuel testin aksine bilinmeyen güvenlik zafiyetlerini tam olarak saptama kapasitesine sahiptir. Yüzlerce açık kaynak projeyi otomatik olarak test etmek amacıyla bir altyapı kurmak için yatırım yaptık. OSS-Fuzz bugün düzenli kod taramaları gerçekleştiriyor ve daha fazla hata sınıfı tespit etmek için sürekli yenilik yapıyor.

Fuzz testi tarafından altı dilde 800'den fazla kritik açık kaynak projesi tarandı.

Sektör Yatırımlarımız ve Önemli Adımlarımız

2020 AĞUSTOS
Açık kaynak yazılım güvenliğine rehberlik etmek ve açık kaynak yazılım güvenliğini geliştirmek için **Açık Kaynak Güvenlik Vakfı'na (OpenSSF) katıldık.**

2021 MAYIS VE HAZİRAN
14028 sayılı Beyaz Saray Başkanlık Kararnamesi'ne uygun olarak **OSS en iyi uygulamalarını oluşturduk** ve yazılım tedarik zinciri güvenlik standartları konusunda rehberlik sağladık.

HAZİRAN
Google'ın dâhilî güvenlik çerçevesini dışa açan ve herkesin daha güvenli yazılımlar oluşturmasına olanak sağlayan **OpenSSF ile birlikte SLSA'yı yayınladık.**

AĞUSTOS
Güvenlik açıklarını bulmak ve düzeltmek için geliştiricilerle iş birliği yapmak dâhil **OSS'yi iyileştirmek ve korumak için 100 milyon $ taahhüt ettik.**

2022 MAYIS
Güvenliklerini iyileştirmek için doğrudan açık kaynak projeleriyle çalışmak üzere tam zamanlı geliştiricilerden oluşan bir ekip tahsis ederek **DC Zirvesi sırasında Google'ın Açık Kaynak Bakım Ekibini duyurduk.**

MAYIS
Google'ın kullandığı güvenilir açık kaynak paketlerinin geliştirici iş akışlarına dâhil edilmesine yardımcı olan **Garantili Açık Kaynak Yazılım ürününü duyurduk.**

Bugün kamu kuruluşlarının ve özel kuruluşların güvende kalmasına yardımcı olabilecek Google tarafından önerilen uygulamalar:

- Yazılım tedarik zinciri güvenliğini geliştirmek için SLSA'yı uygulamak
- Yazılımınızın gerçekliğini Sigstore kullanarak kriptografik olarak imzalamak ve doğrulamak
- OSS-Fuzz ve OSV.dev ile açıklık keşfetme, izleme ve önceliklendirmeyi otomatikleştirmek
- Bağlılıklarınızla güvenlik riskini otomatik olarak değerlendirmek için Skor kartları kullanmak

Yaklaşımımız

Yazılım, sadece en zayıf halka kadar güvenlidir. Açık kaynak ekosistemin tamamının güvenliğini artırmak için uzmanlığımızı ve mali kaynaklarımızı yatırıyoruz. Geliştirme ve güvenlik uzmanlarından oluşan ekibimiz aşağıdaki yollardan daha fazla kamu ve özel sektör kuruluşunu koruyabileceğimize inanıyor:

Ekiplerimiz, güvenlik açıklarını saptamak için sürekli olarak tarama yaparak, analizler gerçekleştirerek ve fuzz testi yaparak ürün yaşam döngüsünün her aşamasını denetler.

Açık interneti destekleriz, bildiklerimizi geliştirici topluluğu ile paylaşırız ve kamunun ve işletmelerin kullanımı için internetin güvenli olmasını sağlarız.

Sofistike tehditleri saptayarak, ileri otomatikleştirilmiş araçlar sağlayarak ve bir adım önde olarak geleceğin güvenliğini geliştiriyoruz.

Açık kaynak yazılımın korunması ortak bir sorumluluktur ve bu acil, kritik problemle ilgili olarak iş birliğine devam etmekte kararlıyız. g.co/security/gosst

Kaynaklar: 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.Bilgimizi paylaşmak (ör. SLSA'yı yayınlamak, OpenSSF'ye rehberlik etmek), yalnızca Google'ın değil, yazılım üreten herkesin Google'ın deneyiminden ve zaman içinde test edilmiş güvenlik uygulamalarından yararlanabileceği anlamına gelir. 5. SLSA, kuruluşların yazılım geliştirme süreçlerinin güvenliğini artırmalarına yardımcı olabilecek bir dizi uygulamadır. Siber güvenliğe ilişkin Başkanlık Kararnamesi'ne yanıt olarak hükümet tarafından ortaya konulan gerekliliklerı içeren, ABD hükümetinin Güvenli Yazılım Geliştirme Çerçevesinin gerekliliklerinin yerine getirilmesine yardımcı olur. Bu, yazılımı herkes için daha güvenli hâle getirmek için federal yönergelere nasıl uyacakları konusunda kuruluşların rehberliğe sahip olacağı anlamına gelir.