Kaspersky Açık Kaynak Yazılım Tehditleri Veri Akışı

kaspersky geleceği yakalayın

Yazılım tedarik zinciri saldırıları

Bu saldırı türünde, siber suçlular bir yazılım satıcısının sistemlerini veya yazılım geliştirme araçlarını tehlikeye atarak, müşterilere dağıtılmadan önce yazılıma kötü amaçlı kod veya kötü amaçlı yazılım ekler.

Kaspersky Açık Kaynak Yazılım Tehditleri Veri Akışı

Siber tehditler sürekli gelişiyor ve giderek daha karmaşık hale geliyor, bu da işletmelerin korunmasını zorlaştırıyor. Kaspersky Açık Kaynak Yazılım Tehditleri Veri Akışı, tehditler ve güvenlik açıkları hakkında güncel bilgiler sağlayarak işletmelerin ağlarını, uç noktalarını ve kritik verilerini korumalarına olanak tanır. Kaspersky Açık Kaynak Yazılım Tehditleri Veri Akışı, gizli tehditlerin algılanması için geliştirmede kullanılan açık kaynak bileşenlerinin izlenmesine yönelik DevSecOps süreçlerine dâhil edilmek üzere tasarlanmıştır.

Güvenliğe yeni bir bakış açısı

Çoğu yazılım geliştiricisi, geliştirme döngülerine açık kaynaklı yazılım paketlerini dâhil eder ve bu paketlerin bütünlüğüne güvenmeye yatkındır.

Siber tehditlerin sayısı ve şiddeti artmaya devam ettikçe, klasik DevOps yazılım geliştirme metodolojisi, DevSecOps olarak bilinen daha güvenlik bilinçli bir yaklaşıma doğru kaymaya başladı. Bu yaklaşım, ilk planlama ve tasarım aşamalarından geliştirme, test ve sonrasına kadar güvenlik uygulamalarının hayata geçirilmesini desteklemektedir. Bu yaklaşım, geliştirme döngüsünde kullanılan tüm açık kaynak kodlu yazılımlar için de geçerli olmalıdır.

Kaspersky, bu güvenlik öncelikli yaklaşımın açık kaynaklı yazılımlara uygulanmasına yardımcı olmak için değerli bir veri akışı tasarladı: Kaspersky Açık Kaynak Yazılım Tehditleri Veri Akışı. Bilinen tüm açık kaynak paketlerindeki tehditleri ve güvenlik açıklarını ortaya çıkaran, ikili olmayan, yalnızca metin içeren bir veri kümesidir.

Tehdit türleri

Kaspersky Açık Kaynak Yazılım Tehditleri Veri Akışı aşağıdaki tehdit türlerini kapsar:

Belirli bölgelerde işlevselliği değiştirilmiş güvenliği ihlal edilmiş paketler

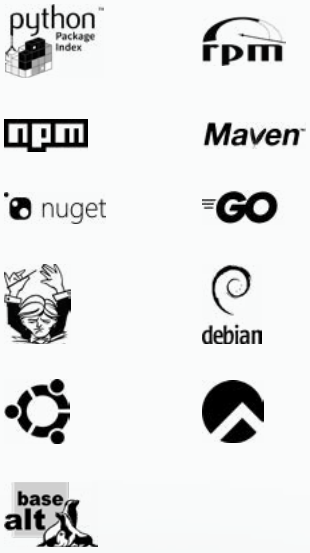
Kriptominerler, bilgisayar korsanlığı araçları vb. gibi potansiyel olarak tehlikeli yazılımlar içeren paketler.

Siyasi mesajlar içeren güvenliği ihlal edilmiş paketler

Güvenlik açıkları içeren paketler

Kötü amaçlı kod içeren paketler

Paket yöneticileri



Güvenlik açığı danışmanları

Akış içeriği

Paket yöneticileri

Akış, depoların düzenli olarak tarandığı aşağıdaki paket yöneticilerinden* gelen şu paketler hakkında bilgiler sağlar:
Pypi, Npm, NuGet, Maven, Composer, Go, Rpm, Debian.

Güvenlik açığı danışmanları

Tüm depolardaki tüm paketler aşağıdaki güvenlik açığı danışmanlıklarıyla otomatik olarak eşleştirilir: GitHub Güvenlik Danışmanlığı, CVE MITRE, Debian, Güvenlik Danışmanlığı, CentOS Güvenlik Uyarıları, RedHat Güvenlik Danışmanlığı (yalnızca bu danışmanlığa çapraz bağlantılar sağlanır).

Bağlam

Paket listesinin yanı sıra aşağıdaki faydalı içerik de sağlanmaktadır:

Güvenlik açıkları için:

- Ekosistem ile bağlantı
- Sistem etkisi
- Güvenlik açığı bulunan sürümlerin listesi
- Otomasyon için savunmasız sürümler CPE/PURL
- Yamalanmış güvenlik açıkları ile önerilen sürümlerin listeleri
- İşletim sistemi sürümleri desteği (*nix paketleri için)
- Güvenlik açığı danışmanlıklarına çapraz bağlantılar
- Şu anda serbest olarak kullanılan açıkların karmaları

Kötü amaçlı ve güvenliği ihlal edilmiş paketler için:

- Ekosistem ile bağlantı
- Sistem etkisi: kötü amaçlı yazılım, hacktool, diğer
- Şiddet
- Güvenliği ihlal edilmiş paket sürümleri
- Güvenliği ihlal edilmiş paket sürümlerinin karmaları
- CWE (Ortak Zayıflık Numaralandırma): şimdilik sadece kötü amaçlı yazılım paketleri için

İş Değeri

Aşağıdakileri yapmalarını sağlayarak kuruluşlara önemli iş değeri sağlanır:

Tehdit Algılamasının İyileştirilmesi

Açık kaynaklı yazılımlarla ilgili en son siber tehditler ve güvenlik açıkları hakkında gerçek zamanlı istihbarat sağlanması. Bu, kurumların tehdit algılama yeteneklerini geliştirmelerini ve potansiyel saldırıları zarar vermeden önce tespit etmelerini sağlar.

Olaya Müdahaleyi Geliştirme

Kuruluşların tehdide hızlı ve etkili bir şekilde yanıt vermesine yardımcı olacak değerli bilgiler sağlayın. Bu, olayın etkisini en aza indirmeye ve olaya müdahale için gereken süreyi ve kaynakları azaltmaya yardımcı olabilir.

Güvenlik Duruşunun Güçlendirilmesi

Kuruluşların kullandıkları açık kaynaklı yazılımlarla ilgili en son güvenlik tehditleri ve güvenlik açıkları hakkında bilgi sahibi olmalarına yardımcı olun. Bu bilgiler, kuruluşların güvenlik açıklarını zamanında tespit edip gidermesine yardımcı olarak siber suçlular tarafından istismar edilme riskini azaltabilir.

Güvenlik Risklerini Azaltma

Kuruluşların açık kaynaklı yazılım kullanımıyla ilişkili güvenlik risklerini azaltmalarına yardımcı olun. Bu, kuruluşun kritik verilerinin, fikri mülkiyetinin ve itibarının korunmasına yardımcı olabilir.

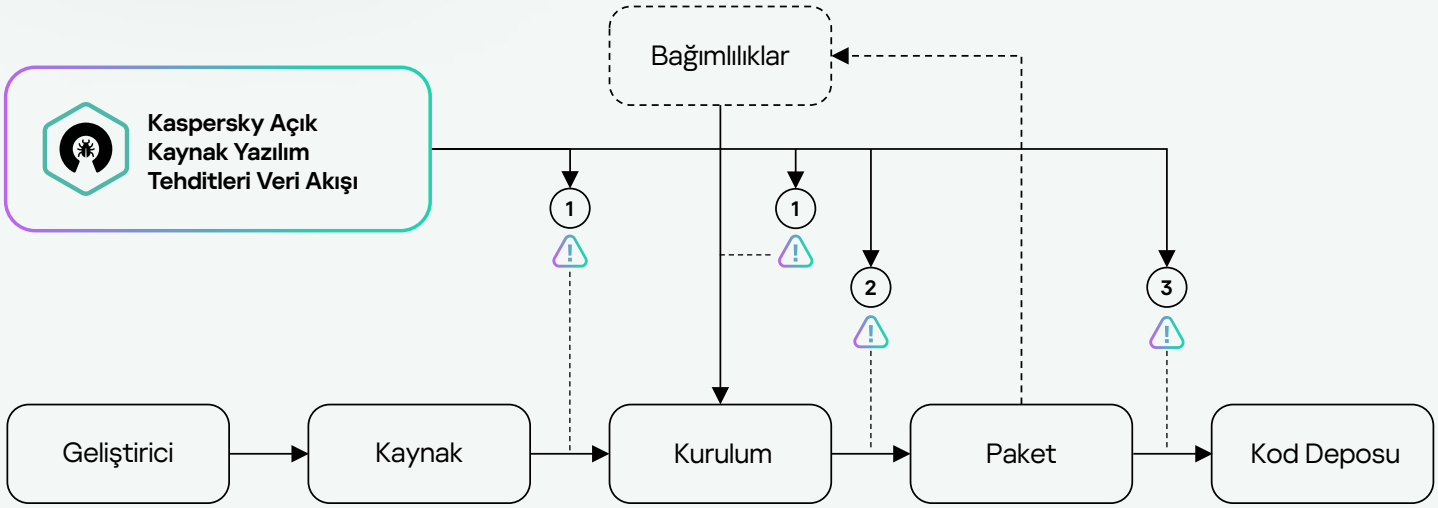
Zaman ve Paradan Tasarruf

Kuruluşların açık kaynaklı yazılımlarla ilgili en son güvenlik tehditleri ve güvenlik açıkları hakkında bilgi sahibi olmaları için uygun maliyetli ve verimli bir yol sağlayın. Bu, kuruluşların kendi tehdit istihbarat sistemlerini oluşturma ve sürdürme konusunda zamandan ve paradan tasarruf etmelerine yardımcı olabilir.

Akış JSON formatında teslim edilir

Kullanım örnekleri

Kaspersky Açık Kaynak Yazılım Tehditleri Veri Akışı için önerilen kullanım örneği şu şekildedir: Akıştaki paketlerin tanımlayıcısının, paket adı, paket sürümü vb. gibi bir veya birkaç parametreye dayalı olarak geliştirmede kullanılan paketlerle eşleştirilmesi.



Entegrasyon noktaları

1

Bir açık kaynak geliştiricisi tarafından depolardan paket indirme aşamasında (entegrasyon noktası - temsilci depo).

2

Sorun yaratabilecek bağımlı paketlerin kontrol edilmesi de dâhil olmak üzere, kaynak kodun geliştiricisi tarafından derleme aşamasında (entegrasyon noktası - birleştirme hattı).

3

Kaynak kodun depoda yayınlanması aşamasında (entegrasyon noktası - yayınlama mekanizması)

Sorunlu bir paketin tespit edilmesi durumunda kurum tarafından benimsenen politikaya uygun olarak hareket edilmesi önerilir (geliştiricinin bilgilendirilmesi, risk tedavisi, engelleme vb.)

Kaspersky Threat Intelligence

Daha fazla bilgi edinin

www.kaspersky.com.tr

#kaspersky
#geleceğiyakalayın