Kaspersky Open Source Software Threat Data Feeds

kaspersky BRING ON THE FUTURE

Ataques a cadeias de suprimentos

Nesse tipo de ataque, criminosos cibernéticos comprometem os sistemas de um fornecedor de software ou ferramentas de desenvolvimento de software, inserindo código malicioso ou malware no software antes de distribuí-lo aos clientes.

Kaspersky Open Source Software Threat Data Feeds

As ameaças cibernéticas estão em constante evolução e se tornando cada vez mais sofisticadas, tornando mais difícil para as empresas se manterem protegidas. O Kaspersky Open Source Software Threats Data Feed fornece informações atualizadas sobre ameaças e vulnerabilidades, permitindo que as empresas protejam suas redes, endpoints e dados críticos. O feed de dados de ameaças de software de código aberto Kaspersky® foi projetado para ser incluso nos processos DevSecOps para monitorar os componentes de código aberto utilizados na detecção de ameaças que podem estar ocultas neles.

Uma nova abordagem à segurança

A maioria dos desenvolvedores de software inclui pacotes de software de código aberto em seu ciclo de desenvolvimento e tende a confiar na integridade desses pacotes.

À medida que o número e a gravidade das ameaças cibernéticas continuam a aumentar, a clássica metodologia DevOps de desenvolvimento de software começou a se deslocar para uma abordagem mais consciente da segurança, conhecida como DevSecOps. Essa abordagem defende a implementação de práticas de segurança desde as fases iniciais de planejamento e design até o desenvolvimento, teste e além. Essa mentalidade deve se aplicar a todo o software de código aberto usado no ciclo de desenvolvimento também.

A Kaspersky projetou um feed de dados valioso para ajudar a aplicar essa abordagem de segurança em primeiro lugar ao software de código aberto: Kaspersky Open Source Software Threats Data Feed. É um conjunto de dados apenas de texto, sem binários, que revela ameaças e vulnerabilidades em todos os pacotes de código aberto conhecidos.

Tipos de ameaças

O Kaspersky Open Source Software Threats Data Feed abrange os seguintes tipos de ameaças:

Pacotes comprometidos com funcionalidade alterada em determinadas regiões.

Pacotes contendo software potencialmente perigoso, como criptomineradores, ferramentas de hacking, etc.

Pacotes comprometidos contendo mensagens políticas

Pacotes com vulnerabilidades

Pacotes Open Source com códigos maliciosos

Gerenciadores de pacotes





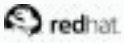


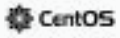




Avisos de vulnerabilidade







Conteúdo do feed

Gerenciadores de pacotes

O feed fornece informações sobre pacotes dos seguintes gerenciadores de pacotes*, cujos repositórios são verificados regularmente: Pypi, Npm, NuGet, Maven, Composer, Go, Rpm, Debian.

Avisos de vulnerabilidade

Todos os pacotes de todos os repositórios são automaticamente comparados com os seguintes avisos de vulnerabilidade: Aviso de Segurança do GitHub, CVE MITRE, Aviso de Segurança do Debian, Alertas de Segurança do CentOS, Aviso de Segurança do RedHat (apenas links cruzados para este aviso são fornecidos).

Contexto

Junto com a lista de pacotes, também é fornecido o seguinte contexto útil:

Para vulnerabilidades:

- Conexão ao ecossistema
- Impacto no sistema
- Lista de versões vulneráveis
- Versões vulneráveis CPE/PURL para automação
- Listas de versões recomendadas com vulnerabilidades corrigidas
- As versões do sistema operacional oferecem suporte (para pacotes *nix)
- Links cruzados para avisos de vulnerabilidade
- Hashes de exploits atualmente usados na natureza

Para pacotes maliciosos e comprometidos:

- Conexão ao ecossistema
- Impacto no sistema: malware, ferramenta de hack, outros
- Gravidade
- Versões comprometidas do pacote
- Hashes das versões comprometidas dos pacotes
- CWE (Common Weakness Enumeration): por enquanto, apenas para pacotes de malware

Valor de negócio

Fornecer valor significativo para as organizações, permitindo que elas:

Aprimore a detecção de ameaças

Fornecer inteligência em tempo real sobre as últimas ameaças cibernéticas e vulnerabilidades relacionadas ao software de código aberto. Isso permite que as organizações melhorem suas capacidades de detecção de ameaças e detectem possíveis ataques antes que possam causar danos.

Melhore a resposta a incidentes

Fornecer informações valiosas para ajudar as organizações a responder rapidamente e de forma eficaz à ameaça. Isso pode ajudar a minimizar o impacto do incidente e reduzir o tempo e os recursos necessários para a resposta ao incidente.

Fortalecer a postura de segurança

Ajudar as organizações a se manterem informadas sobre as últimas ameaças de segurança e vulnerabilidades relacionadas ao software de código aberto que elas utilizam. Essas informações podem ajudar as organizações a identificar e remediar vulnerabilidades de forma oportuna, reduzindo o risco de exploração por cibercriminosos.

Reduzir os riscos de segurança

Ajudar as organizações a reduzir os riscos de segurança associados ao uso de software de código aberto. Isso pode ajudar a proteger os dados críticos da organização, propriedade intelectual e reputação.

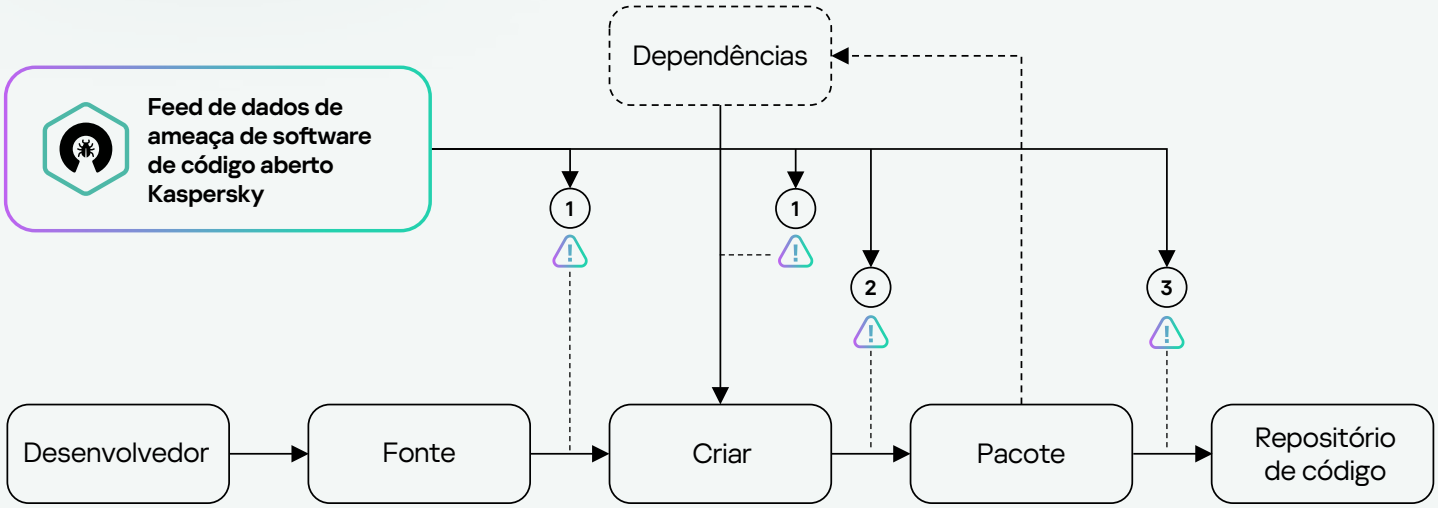
Economize tempo e recursos

Fornecer uma maneira econômica e eficiente para as organizações se manterem informadas sobre as últimas ameaças de segurança e vulnerabilidades relacionadas ao software de código aberto. Isso pode ajudar as organizações a economizar tempo e dinheiro na construção e manutenção de seus próprios sistemas de inteligência de ameaças.

O feed é entregue no formato JSON

Use casos

O caso de uso recomendado para o Kaspersky Open Source Software Threats Data Feed é o seguinte: comparar o identificador de pacotes do feed com os pacotes usados no desenvolvimento com base em um ou vários parâmetros, como nome do pacote, versão do pacote etc.



Pontos de integração

1

Na fase de download de pacotes de repositórios por um desenvolvedor de código aberto (ponto de integração — proxy de repositório).

2

Na fase de compilação pelo desenvolvedor do código-fonte, incluindo a verificação de pacotes dependentes, o que também pode ser problemático (ponto de integração - linha de montagem).

3

Na etapa de publicação do código-fonte no repositório (ponto de integração - mecanismo de publicação)

A recomendação em caso de detecção de um pacote problemático é agir de acordo com a política adotada pela organização (notificação do desenvolvedor, tratamento de riscos, bloqueio etc.).

Kaspersky Threat Intelligence

Saiba mais

www.kaspersky.com.br

#kaspersky
#bringonthefuture