Kaspersky Open Source Software Threats Data Feed

kaspersky bring on the future

Attacchi alla supply chain del software

In questo tipo di attacco, i criminali informatici compromettono i sistemi o gli strumenti di sviluppo software di un fornitore, inserendo codice dannoso o malware all'interno del software prima che venga distribuito ai clienti.

Kaspersky Open Source Software Threats Data Feed

Le minacce informatiche si evolvono costantemente e diventano sempre più sofisticate, rendendo più difficile per le aziende rimanere protette. Kaspersky Open Source Software Threats Data Feed fornisce informazioni aggiornate su minacce e vulnerabilità, consentendo alle aziende di proteggere le reti, gli endpoint e i dati critici. Kaspersky Open Source Software Threats Data Feed è progettato per essere incluso nei processi DevSecOps per il monitoraggio dei componenti open source utilizzati nello sviluppo software, in modo da rilevare le minacce nascoste.

Nuovo approccio alla sicurezza

La maggior parte degli sviluppatori di software include pacchetti software open-source nel ciclo di sviluppo e in genere si fida dell'integrità di questi pacchetti.

Con il continuo aumento del numero e della gravità delle minacce informatiche, la classica metodologia DevOps di sviluppo del software ha iniziato a orientarsi a un approccio più attento alla sicurezza, noto come DevSecOps. Questo approccio prevede l'applicazione di pratiche di sicurezza a partire dalle fasi iniziali di pianificazione e progettazione, fino allo sviluppo, al testing e oltre. Questa mentalità deve essere applicata anche a tutto il software open-source utilizzato nel ciclo di sviluppo.

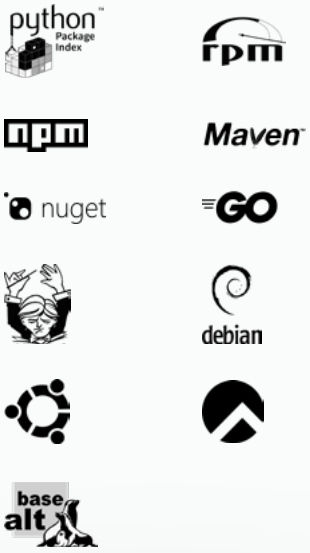
Kaspersky ha progettato uno specifico feed di dati che aiuta ad applicare questo approccio orientato alla sicurezza anche al software open-source grazie a Kaspersky Open Source Software Threats Data Feed. Si tratta di un set di dati di solo testo e non binari che rivela le minacce e le vulnerabilità di ogni pacchetto open-source conosciuto.

Tipi di minacce

Kaspersky Open Source Software Threats Data Feed copre le tipologie di minacce seguenti:

- Pacchetti compromessi con funzionalità alterate in alcune aree geografiche
- Pacchetti contenenti software potenzialmente pericolosi come cryptominer, strumenti di hacking e così via
- Pacchetti compromessi contenenti messaggi politici
- Pacchetti con vulnerabilità
- Pacchetti con codice dannoso

Gestori di pacchetti



Servizi di consulenza sulle vulnerabilità

Contenuto del feed

Gestori di pacchetti

Il feed fornisce informazioni sui pacchetti dei seguenti gestori*, i cui repository vengono scansionati regolarmente:
Pypi, Npm, NuGet, Maven, Composer, Go, Rpm, Debian.

Servizi di consulenza sulle vulnerabilità

Tutti i pacchetti di tutti i repository vengono automaticamente confrontati con gli avvisi dei seguenti servizi di consulenza sulle vulnerabilità: GitHub Security Advisory, CVE MITRE, Debian, Security Advisory, CentOS Security Alerts, RedHat Security Advisory (vengono forniti solo i link incrociati a questo servizio).

Contesto

Oltre all'elenco dei pacchetti, viene fornito anche il seguente contesto che potrà essere utile durante le fasi di analisi:

Per le vulnerabilità:

- Connessione all'ecosistema
- Impatto sul sistema
- Elenco di versioni vulnerabili
- CPE/PURL delle versioni vulnerabili per l'automazione
- Elenco di versioni consigliate con patch per le vulnerabilità
- Supporto delle versioni del sistema operativo (per i pacchetti *nix)
- Collegamenti incrociati ai servizi di consulenza per le vulnerabilità
- Hash degli exploit attualmente usati

Per i pacchetti dannosi e compromessi:

- Connessione all'ecosistema
- Impatto sul sistema: malware, strumenti di hacking, altro
- Gravità
- Versioni dei pacchetti compromessi
- Hash delle versioni dei pacchetti compromessi
- CWE (Common Weakness Enumeration): per il momento, solo per i pacchetti di malware.

Valore aziendale

Ecco come assicurare alle organizzazioni un grande valore a livello aziendale:

Migliorare la threat detection

Fornite informazioni in tempo reale sulle minacce informatiche e sulle vulnerabilità più recenti relative al software open-source. In questo modo le organizzazioni saranno in grado di migliorare le loro capacità di threat detection e di individuare i potenziali attacchi prima che possano causare danni.

Migliorare la risposta agli incidenti

Fornite informazioni preziose per aiutare le organizzazioni a rispondere in modo rapido ed efficace alla minaccia. Sarà così possibile ridurre al minimizzo l'impatto dell'incidente e limitare il tempo e le risorse necessarie per rispondere.

Consolidare l'approccio alla sicurezza

Aiutate le organizzazioni a rimanere informate sulle minacce alla sicurezza e sulle vulnerabilità più recenti relative al software open-source utilizzato. Queste informazioni consentono alle organizzazioni di identificare e correggere le vulnerabilità in modo tempestivo, riducendo il rischio di sfruttamento da parte dei criminali informatici.

Ridurre i rischi di sicurezza

Aiutate le organizzazioni a ridurre i rischi per la sicurezza associati all'uso di software open-source. Le organizzazioni saranno così in grado di proteggere i dati critici, la proprietà intellettuale e la loro reputazione.

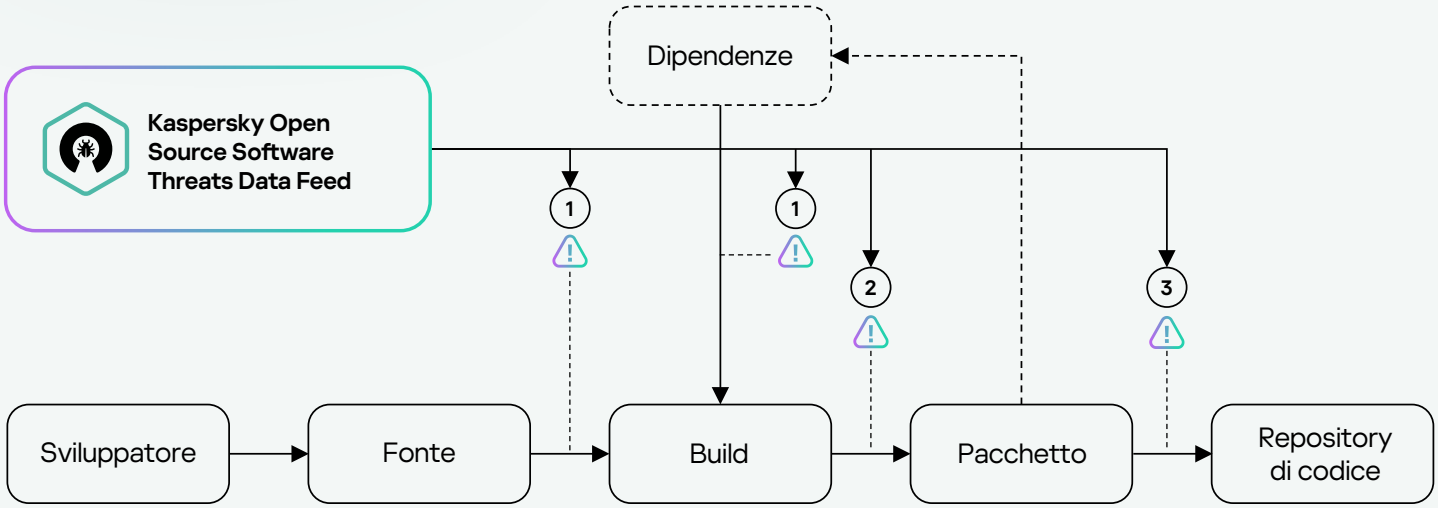
Risparmiare tempo e denaro

Fornite alle organizzazioni un modo conveniente ed efficiente per tenersi informate sulle minacce alla sicurezza e sulle vulnerabilità più recenti relative al software open-source. Le organizzazioni potranno così risparmiare tempo e denaro per la creazione e la gestione dei sistemi di threat intelligence.

Il feed viene fornito in formato JSON

Casi d'uso

Il caso d'uso consigliato per Kaspersky Open Source Software Threats Data Feed è il seguente: confrontare le informazioni contenute sui pacchetti all'interno del feed con quello dei pacchetti utilizzati nelle fasi di sviluppo in base a uno o più parametri, come il nome del pacchetto, la versione e così via.



Punti di integrazione

1

Durante il download dei pacchetti dai repository da parte di uno sviluppatore open-source (punto di integrazione - repository di proxy).

2

Durante la compilazione da parte dello sviluppatore del codice sorgente, incluso il controllo dei pacchetti dipendenti, che possono essere anch'essi problematici (punto di integrazione - catena di montaggio).

3

Durante la pubblicazione del codice sorgente nel repository (punto di integrazione - meccanismo di pubblicazione)

Il consiglio in caso di rilevamento di un pacchetto problematico è di agire in conformità con la politica adottata dall'organizzazione (notifica allo sviluppatore, trattamento del rischio, blocco e così via).

Kaspersky Threat Intelligence

Ulteriori informazioni

www.kaspersky.it

#kaspersky
#bringonthefuture