Kaspersky Open Source Software Threats Data Feed

kaspersky bring on the future

Supply chain-anvallen op de software

Bij dit type aanval hacken cybercriminelen de systemen of softwareontwikkelingstools van een softwareleverancier en voegen ze schadelijke code of malware toe aan de software voordat deze aan klanten wordt geleverd.

Kaspersky Open Source Software Threats Data Feed

Cyberbedreigingen veranderen continue en worden steeds geavanceerder. Hierdoor wordt het lastiger voor bedrijven om beschermd te blijven. Kaspersky Open Source Software Threats Data Feed biedt up-to-date gegevens over bedreigingen en kwetsbaarheden, waardoor bedrijven hun netwerken, endpoints en kritieke gegevens kunnen beschermen. Kaspersky Open Source Software Threats Data Feed is ontworpen om te worden opgenomen in DevSecOps-processen om de open source-componenten te controleren die worden gebruikt tijdens de ontwikkeling om verborgen bedreigingen te detecteren.

Een nieuwe benadering van beveiliging

De meeste softwareontwikkelaars voegen open source-softwarepakketten toe aan hun ontwikkelingscyclus en vertrouwen de integriteit van deze pakketten.

Aangezien het aantal en de ernst van cyberbedreigingen blijft toenemen, verandert de klassieke DevOps-methodologie van softwareontwikkeling naar een meer beveiligingsgerichte aanpak, bekend als DevSecOps. Deze aanpak zorgt dat beveiligingspraktijken worden toegepast vanaf de initiële plannings- en ontwerpfase tot aan de ontwikkelings- en testfase. Deze mentaliteit moet ook worden toegepast voor alle open source-software die wordt gebruikt in de ontwikkelingscyclus.

Kaspersky heeft een waardevolle gegevensfeed ontworpen om deze beveiligingsgerichte aanpak op open source-software toe te passen: Kaspersky Open Source Software Threats Data Feed. Het is een niet-binaire gegevensset met alleen tekst die bedreigingen en kwetsbaarheden binnen elk bekend open source-pakket onthult.

Soorten b edreigingen

De Kaspersky Open Source Software Threats Data Feed pakt de volgende soorten bedreigingen aan:

Gehackte pakketten met aangepaste functionaliteit in bepaalde regio's

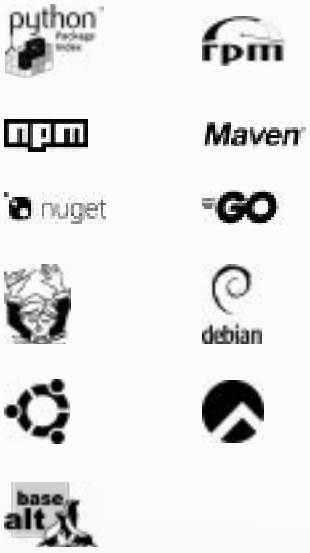
Pakketten die mogelijk gevaarlijke software bevatten, zoals cryptominers, hackingtools, enz.

Gehackte pakketten die politieke berichten bevatten

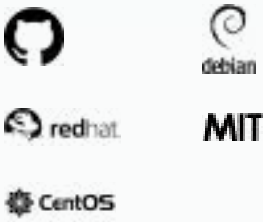
Pakketten met kwetsbaarheden

Pakketten met schadelijke code

Pakketmanagers



Waarschuwingen van kwetsbaarheden



Inhoud van de feed

Pakketmanagers

De feed biedt informatie over pakketten van de volgende pakketmanagers*, waarbij opslagplaatsen regelmatig worden gescand: Pypi, Npm, NuGet, Maven, Composer, Go, Rpm, Debian.

Waarschuwingen van kwetsbaarheden

Alle pakketten van alle opslagplaatsen worden automatisch gematcht met de volgende kwetsbaarheidswaarschuwingen: GitHub Security Advisory, CVE MITRE, Debian, Security Advisory, CentOS Security Alerts, RedHat Security Advisory (er worden alleen cross-links naar deze waarschuwing geboden).

Context

Behalve de lijst met pakketten wordt de volgende nuttige context geboden:

Voor kwetsbaarheden:

- Verbinding met het ecosysteem
- Impact op systemen
- Lijst van kwetsbare versies
- Kwetsbare versies CPE/PURL voor automatisering
- Lijst van aanbevolen versies met gepatchte kwetsbaarheden
- Ondersteuning voor besturingssysteemversies (voor *nix-pakketten)
- Cross-links naar kwetsbaarheidsadviezen
- Hashes van exploits die momenteel worden gebruikt

Voor schadelijke en gehacktepakketten:

- Verbinding met het ecosysteem
- Systeemimpact: malware, hacktool, anders
- Ernst
- Gehackte pakketversies
- Hashes van gehackte pakketversies
- CWE (Common Weakness Enumeration): momenteel alleen voor malwarepakketten

Bedrijfs waarde

Bied aanzienlijke bedrijfswaarde voor organisaties door ze in staat te stellen om:

De bedreigingsdetectie te verbeteren

Informatie te bieden over de nieuwste cyberbedreigingen en kwetsbaarheden die zijn gerelateerd aan open source-software. Dit stelt organisaties in staat om hun mogelijkheden voor bedreigingsdetectie te verbeteren en mogelijke aanvallen te detecteren voordat ze schade kunnen veroorzaken.

Incidentrespons verbeteren

Verstrek waardevolle informatie om organisaties te helpen om snel en effectief op de bedreiging te reageren. Dit kan helpen om de impact van het incident te beperken en de tijd en bronnen te verminderen die nodig zijn voor incidentrespons.

Beveiligingspositie versterken

Help organisaties om op de hoogte te blijven van de nieuwste beveiligingsbedreigingen en kwetsbaarheden die zijn gerelateerd aan de open source-software die ze gebruiken. Deze informatie kan organisaties helpen om kwetsbaarheden tijdig te identificeren en te verhelpen. Dit verkleint het risico op misbruik door cybercriminelen.

Beveiligingsrisico's verminderen

Help organisaties om de beveiligingsrisico's te verminderen die zijn gerelateerd aan het gebruik van open source-software. Dit kan helpen om de kritieke gegevens, het intellectueel eigendom en de reputatie van de organisatie te beschermen.

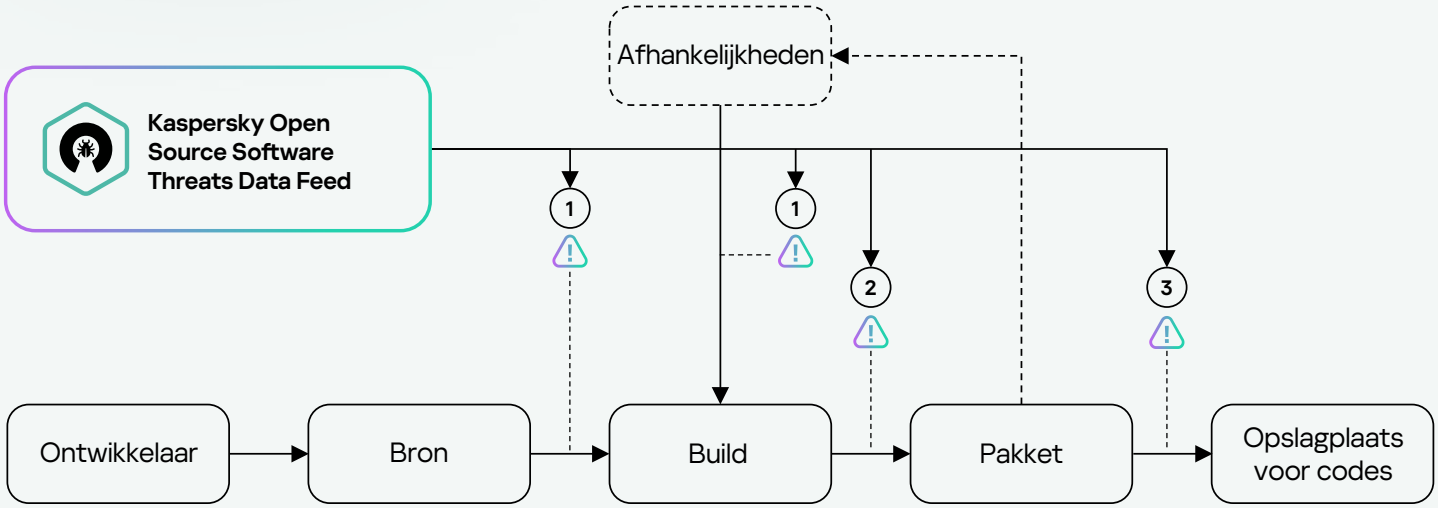
Tijd en geld besparen

Bied een voordelige en efficiënte manier voor organisaties om op de hoogte te blijven van de nieuwste beveiligingsbedreigingen en kwetsbaarheden die zijn gerelateerd aan open source-software. Dit helpt organisaties om tijd en geld te besteden bij het ontwikkelen en behouden van hun eigen bedreigingsinformatiesystemen.

De feed wordt geleverd in een JSON-indeling

Gebruiks scenario's

Het aanbevolen gebruiksscenario van Kaspersky Open Source Software Threats Data Feed is als volgt: match de identifier van de pakketten uit de feed met de pakketten die zijn gebruikt bij ontwikkeling, op basis van één of meerdere parameters, bijvoorbeeld pakketnaam, pakketversie, etc.



Integratie punten

1

Tijdens de fase van het downloaden van pakketten uit opslagplaatsen door een open source-ontwikkelaar (integratiepunt: proxy-repository).

2

Tijdens de fase van samenstelling door de ontwikkelaar van de broncode, waaronder met afhankelijke pakketten, die ook problematisch kunnen zijn (integratiepunt: lopende band).

3

Tijdens de fase van het publiceren van de broncode in de repository (integratiepunt: publicatiemechanisme)

De aanbeveling in het geval van het detecteren van een problematisch pakket is om te handelen in overeenstemming met het beleid dat wordt gehandhaafd door de organisatie (melding van de ontwikkelaar, risicobehandeling, blokkering, enz.).

Kaspersky Threat Intelligence

Meer informatie

www.kaspersky.nl

#kaspersky
#bringonthefuture