Kaspersky Open Source Software Threats Data Feed

kaspersky bring on the future

Software supply chain attacks

In this type of attack, cybercriminals compromise a software vendor's systems or software development tools, inserting malicious code or malware into the software before it is distributed to customers.

Kaspersky Open Source Software Threats Data Feed

Cyberthreats are constantly evolving and becoming increasingly sophisticated, making it harder for businesses to stay protected. Kaspersky Open Source Software Threats Data Feed provides up-to-date information on threats and vulnerabilities, enabling businesses to protect their networks, endpoints, and critical data. Kaspersky Open Source Software Threats Data Feed is designed to be included in DevSecOps processes for monitoring the open source components used in development to detect hidden threats.

A new approach to security

Most software developers include open source software packages in their development cycle, and tend to trust the integrity of these packages.

As the number and severity of cyberthreats continues to rise, the classic DevOps methodology of software development has begun to shift towards a more security-conscious approach, known as DevSecOps. This approach advocates putting security practices into effect from the initial planning and design stages through to development, testing and beyond. This mindset must apply to all open source software used in the development cycle as well.

Kaspersky has designed a valuable data feed to help apply this security-first approach to open source software: Kaspersky Open Source Software Threats Data Feed. It’s a binary-less, text-only data set that reveals threats and vulnerabilities within every known open source package.

Threat types

The Kaspersky Open Source Software Threats Data Feed covers the following threat types:

Compromised packages with altered functionality in certain regions

Packages containing potentially dangerous software such as cryptominers, hacking tools, etc.

Compromised packages containing political messages

Packages with vulnerabilities

Packages with malicious code

Package managers

python Package Index

rpm

npm

Maven

nuget

GO

debian

base alt

Vulnerability advisories

debian

redhat

MITRE

CentOS

Feed content

Package managers

The feed provides information about packages from the following package managers*, which repositories scanned on a regular basis: Pypi, Npm, NuGet, Maven, Composer, Go, Rpm, Debian.

Vulnerability advisories

All packages from all repositories are automatically matched against the following vulnerability advisories: GitHub Security Advisory, CVE MITRE, Debian, Security Advisory, CentOS Security Alerts, RedHat Security Advisory (only cross-links to this advisory are provided).

Context

Along with the list of packages, the following useful context is also provided:

For vulnerabilities:

- Connection to the ecosystem
- System impact
- List of vulnerable versions
- Vulnerable versions CPE/PURL for automation
- Lists of recommended versions with patched vulnerabilities
- OS versions support (for *nix packages)
- Cross-links to vulnerability advisories
- Hashes of exploits currently used in the wild

For malicious and compromised packages:

- Connection to the ecosystem
- System impact: malware, hacktool, other
- Severity
- Compromised package versions
- Hashes of compromised package versions
- CWE (Common Weakness Enumeration): for the moment, only for malware packages

Business value

Provide significant business value to organizations by enabling them to:

Improve Threat Detection

Provide real-time intelligence on the latest cyber threats and vulnerabilities related to open source software. This enables organizations to improve their threat detection capabilities and detect potential attacks before they can do damage.

Enhance Incident Response

Provide valuable information to help organizations respond quickly and effectively to the threat. This can help minimize the impact of the incident and reduce the time and resources required for incident response.

Strengthen Security Posture

Help organizations stay informed about the latest security threats and vulnerabilities related to the open source software they use. This information can help organizations identify and remediate vulnerabilities in a timely manner, reducing the risk of exploitation by cybercriminals.

Reduce Security Risks

Help organizations reduce the security risks associated with using open source software. This can help protect the organization's critical data, intellectual property, and reputation.

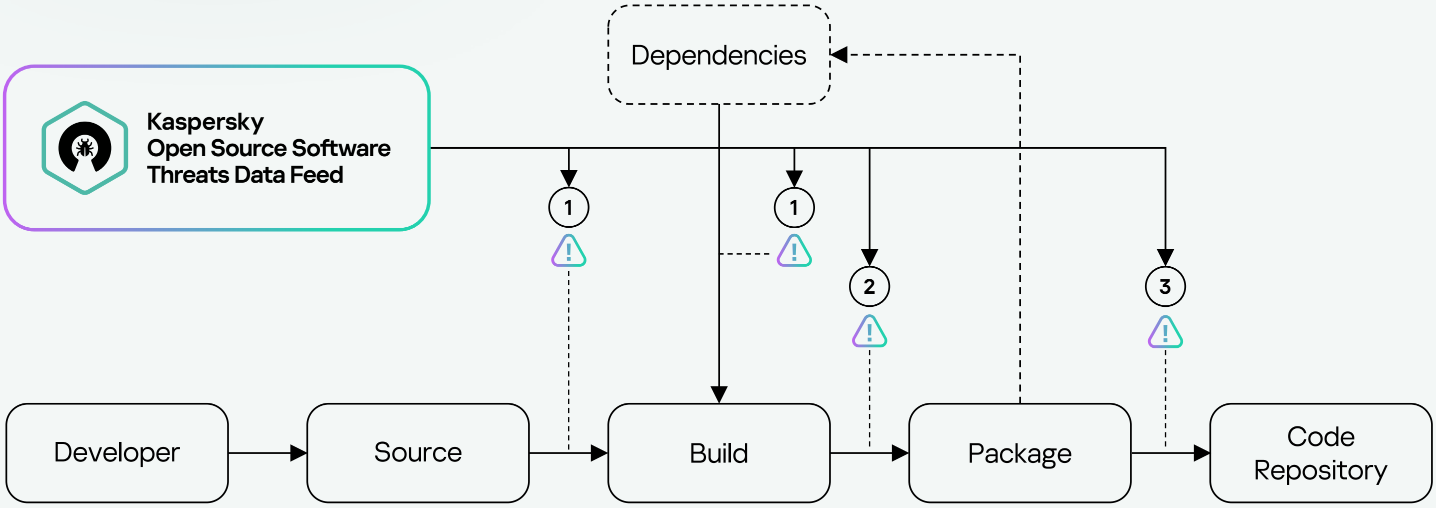
Save Time and Money

Provide a cost-effective and efficient way for organizations to stay informed about the latest security threats and vulnerabilities related to open source software. This can help organizations save time and money on building and maintaining their own threat intelligence systems.

The feed is delivered in JSON format

Use cases

The recommended use case for Kaspersky Open Source Software Threats Data Feed is as follows: match the identifier of packages from the feed against the packages used in development based on one or several parameters. such as package name, package version, etc.



Integration points

1

At the stage of downloading packages from repositories by an open source developer (integration point — proxying repository).

2

At the stage of compilation by the developer of the source code, including with checking dependent packages, which can also be problematic (integration point - assembly line).

3

At the stage of publishing the source code to the repository (integration point — publishing mechanism)

ⓘ The recommendation in case of detecting a problematic package is to act in accordance with the policy adopted by the organization (notification of the developer, risk treatment, blocking, etc.).

Kaspersky Threat Intelligence

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture