



22^a EDIZIONE

When *dependabot* is not enough

Protecting our software supply chain



Edoardo Dusi

Developer Relations Engineer @ SparkFabrik

edoardo.dusi@sparkfabrik.com

@edodusi

@edo@continuousdelivery.social



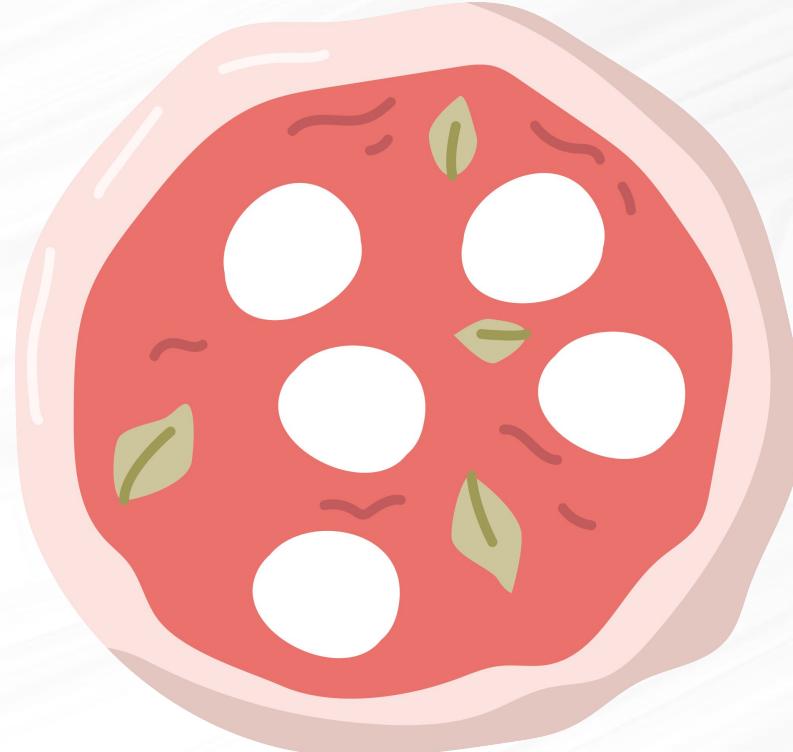
What is the Software Supply Chain



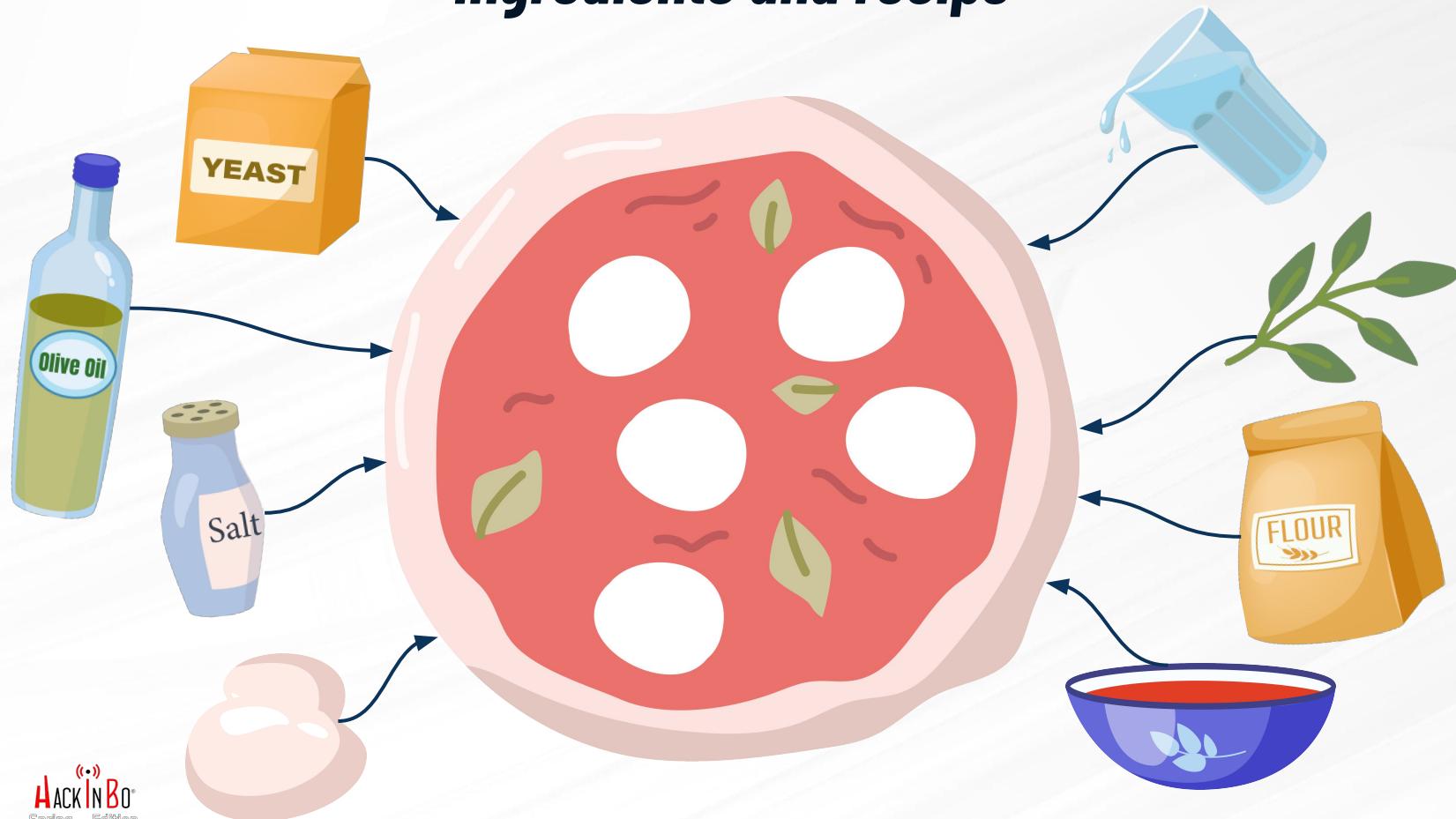
The **software supply chain** refers to the end-to-end process of creating, delivering, and maintaining software applications.



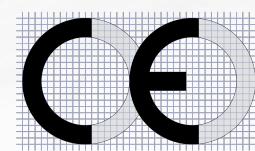
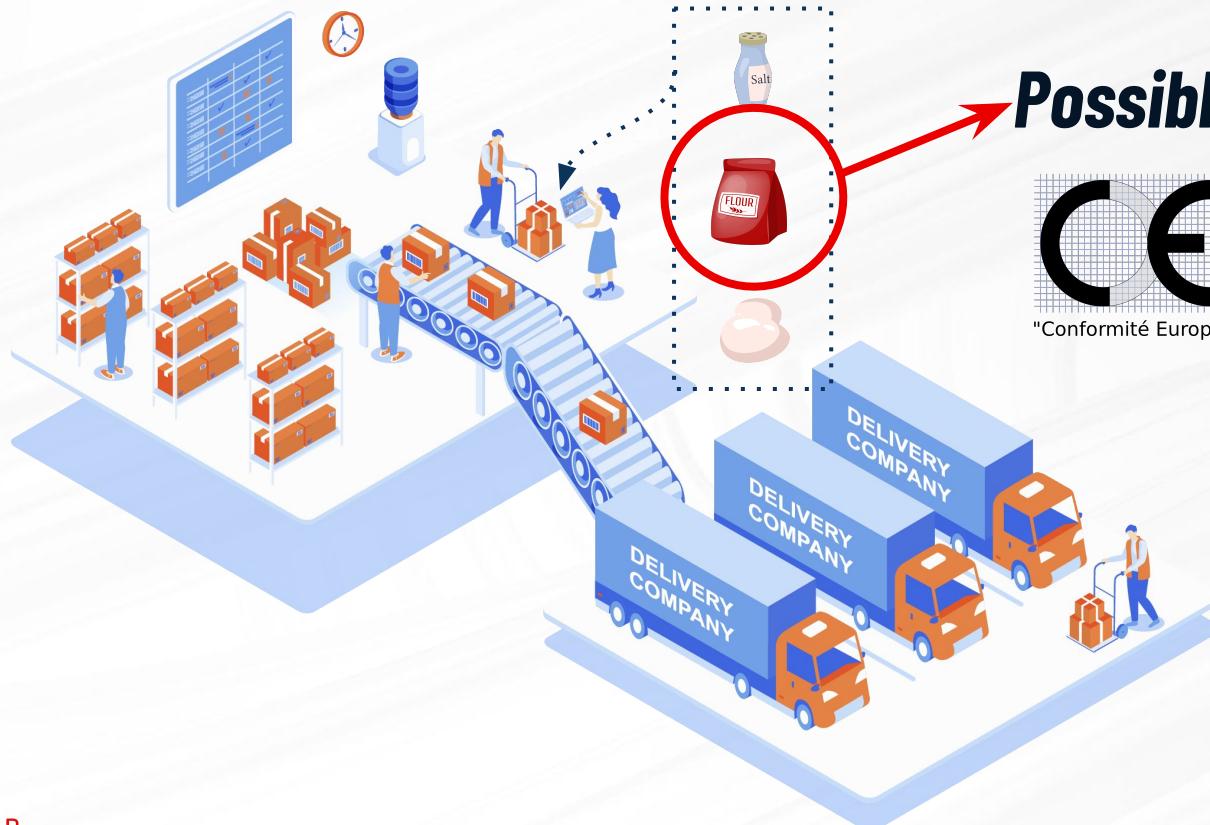
The supply chain of a pizza



Ingredients and recipe



Distributors



"Conformité Européenne"



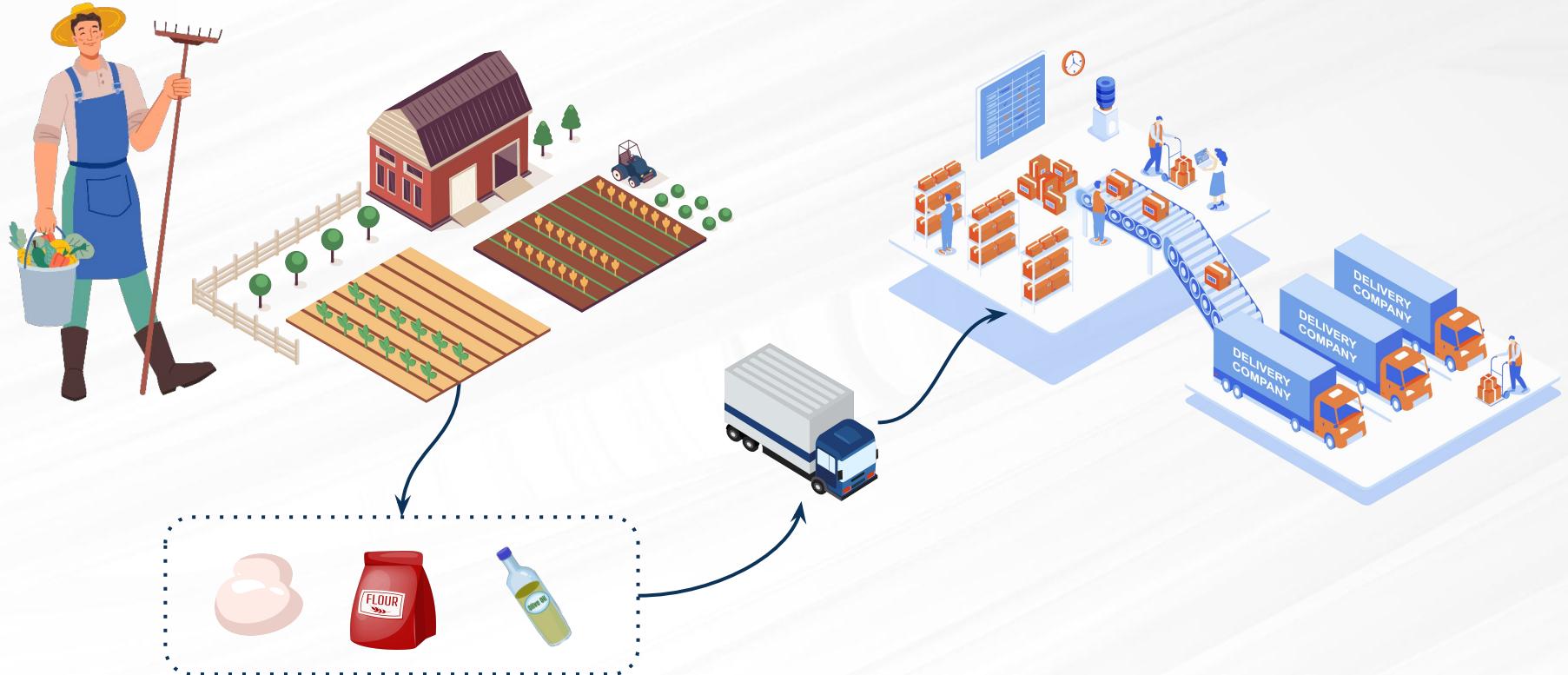
"China Export"



Distribution



Supply Chain



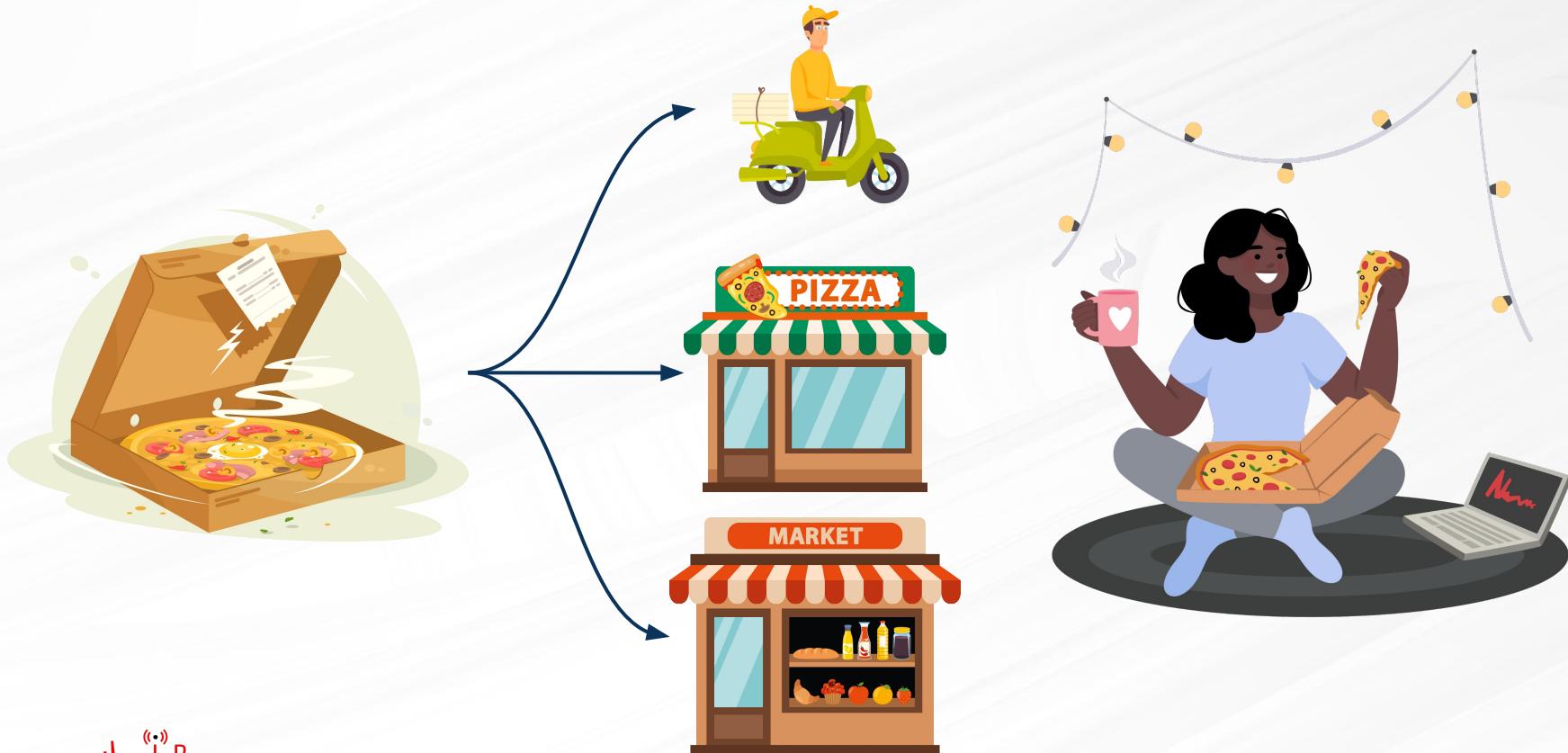
Get ingredients and check receipts

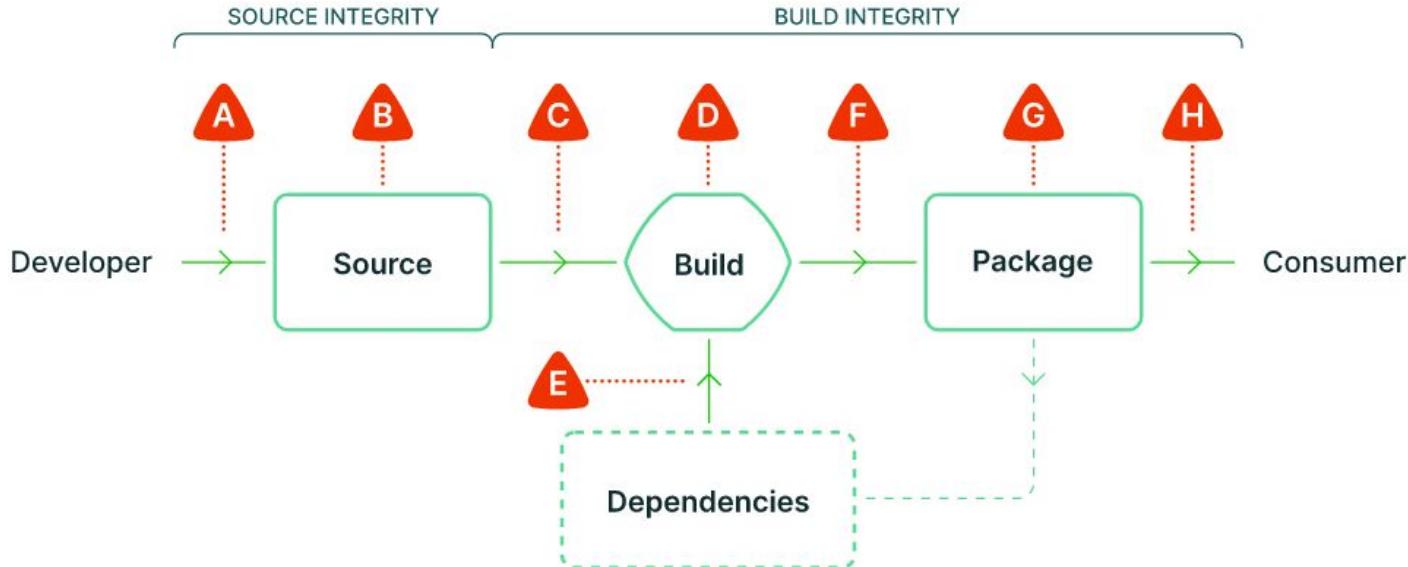


Cooking



Delivery





A Submit unauthorized change

B Compromise source repo

C Build from modified source

D Compromise build process

E Use compromised dependency

F Upload modified package

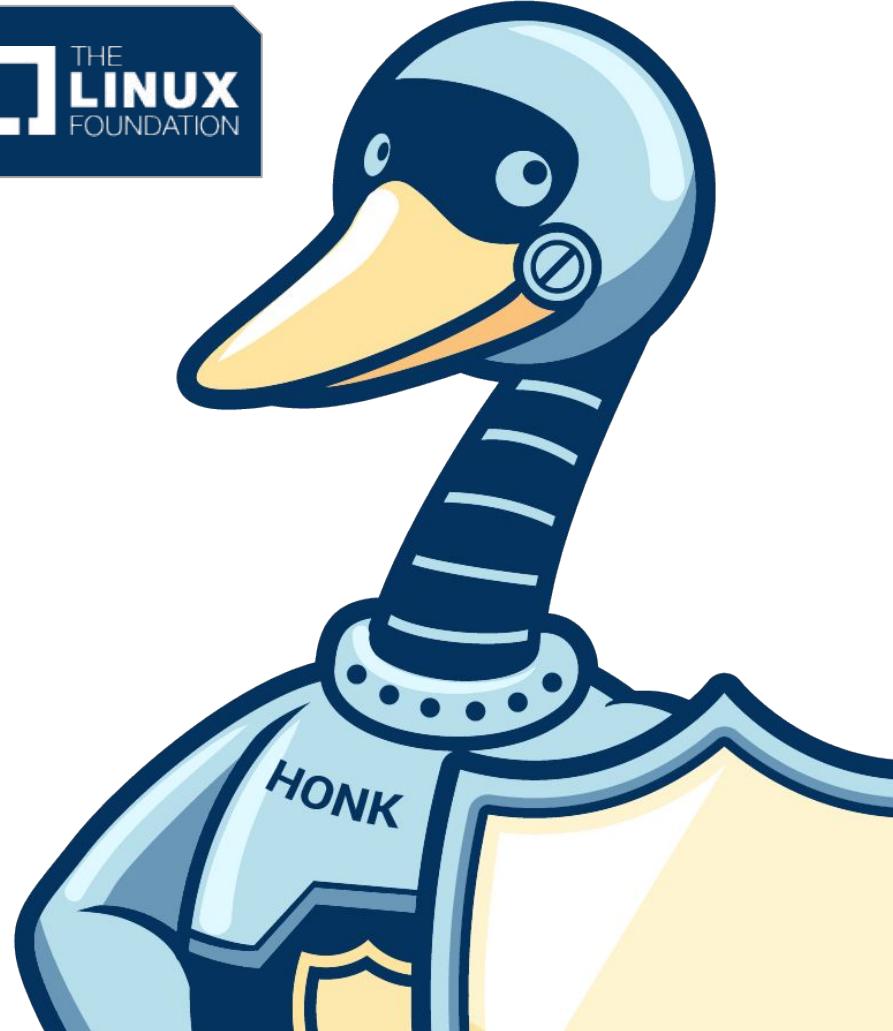
G Compromise package repo

H Use compromised package



Purpose

The OpenSSF is a cross-industry organization that brings together the industry's most important open source security initiatives and the individuals and companies that support them. The OpenSSF is committed to collaboration and working both upstream and with existing communities to advance open source security for all.



Key Components

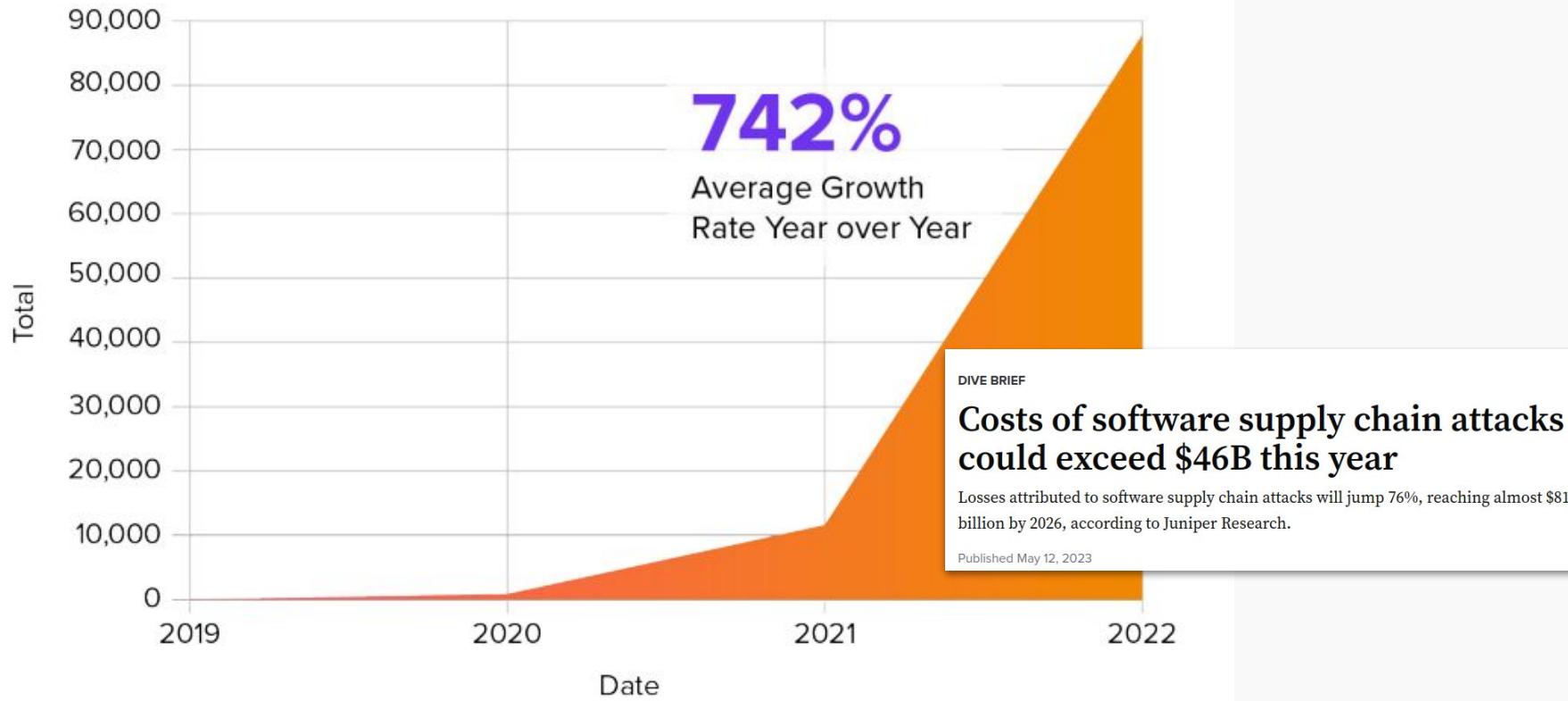
- **Development:** The phase where code is written and applications are built
- **Build and Integration:** Compiling source code, integrating modules, and creating a package
- **Testing:** Unit or E2E testing to identify and fix bugs, ensuring software reliability
- **Deployment:** Deploying software to a server
- **Distribution:** Packaging and delivering software to end users, through physical media or digital channels
- **Updates and Maintenance:** Ongoing efforts to enhance, fix issues, and provide support post-deployment



Importance of Software Supply Chain Security

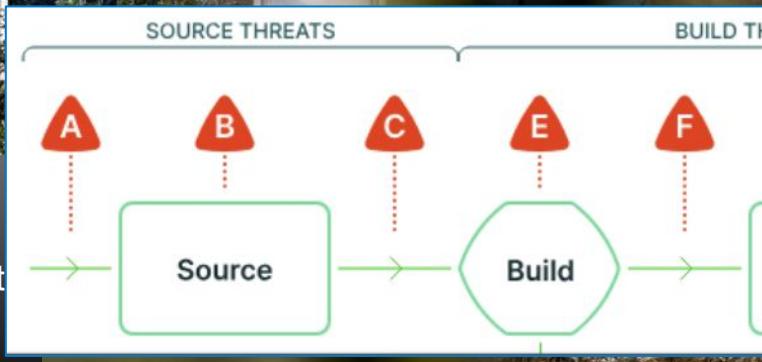


**FIGURE 1.6 NEXT GENERATION SOFTWARE SUPPLY
CHAIN ATTACKS, 2019-2022**

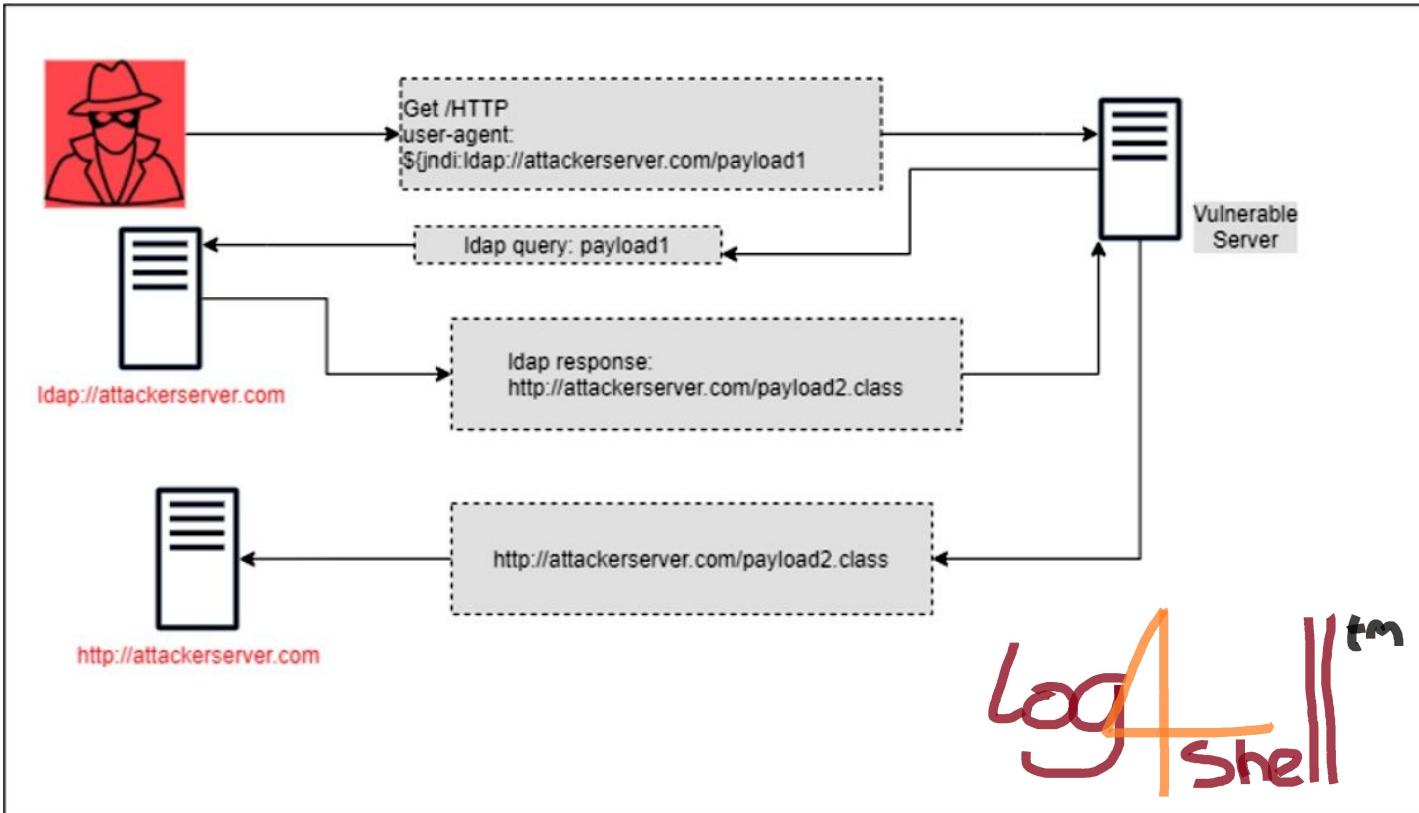


2020

About **18,000 customers** of SolarWinds installed the infected updates, including firms like Microsoft (Cisco, Intel, Deloitte) and top government US agencies like Pentagon, Homeland security, National Nuclear Security etc.



Description of the CVE-2021-44228 vulnerability



NATIONAL CYBERSECURITY STRATEGY

MARCH 2023



CYBER RESILIENCE ACT

New EU cybersecurity rules ensure more secure hardware and software products

#DigitalEU #SecurityUnion #Cybersecurity

#SOTEU

XZ Outbreak (CVE-2024-3094)



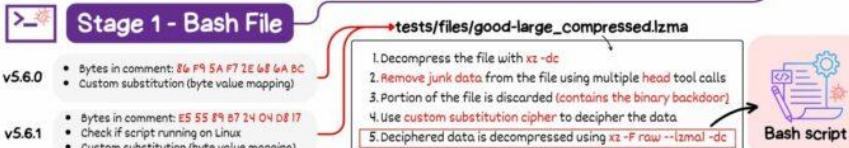
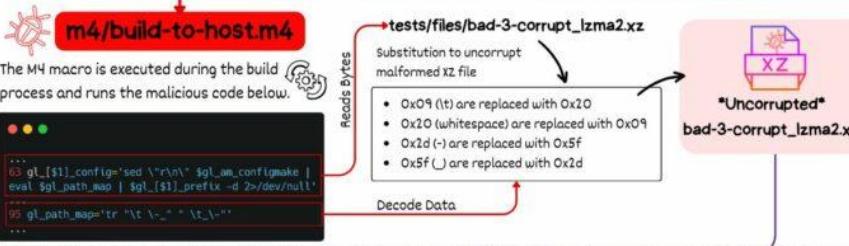
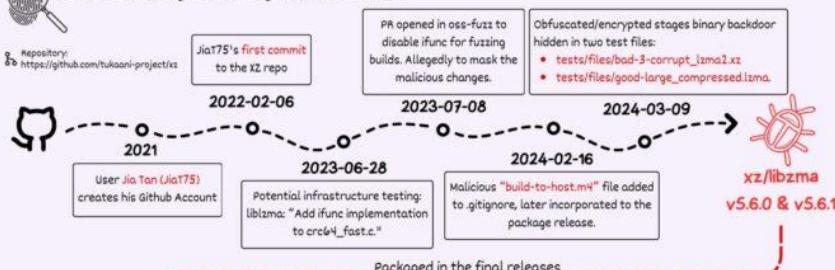
XZ Utils is a collection of open-source tools and libraries for the XZ compression format, that are used for high compression ratios with support for multiple compression algorithms, notably LZMA2.



On Friday 29th of March, Andres Freud (principal software engineer at Microsoft) emailed oss-security informing the community of the discovery of a backdoor in xz/liblzma version 5.6.0 and 5.6.1.

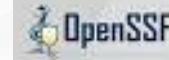


Github Activity Summary (user: JiaT75)



Stage 2 - Bash File

v5.6.1 Extension Mechanism



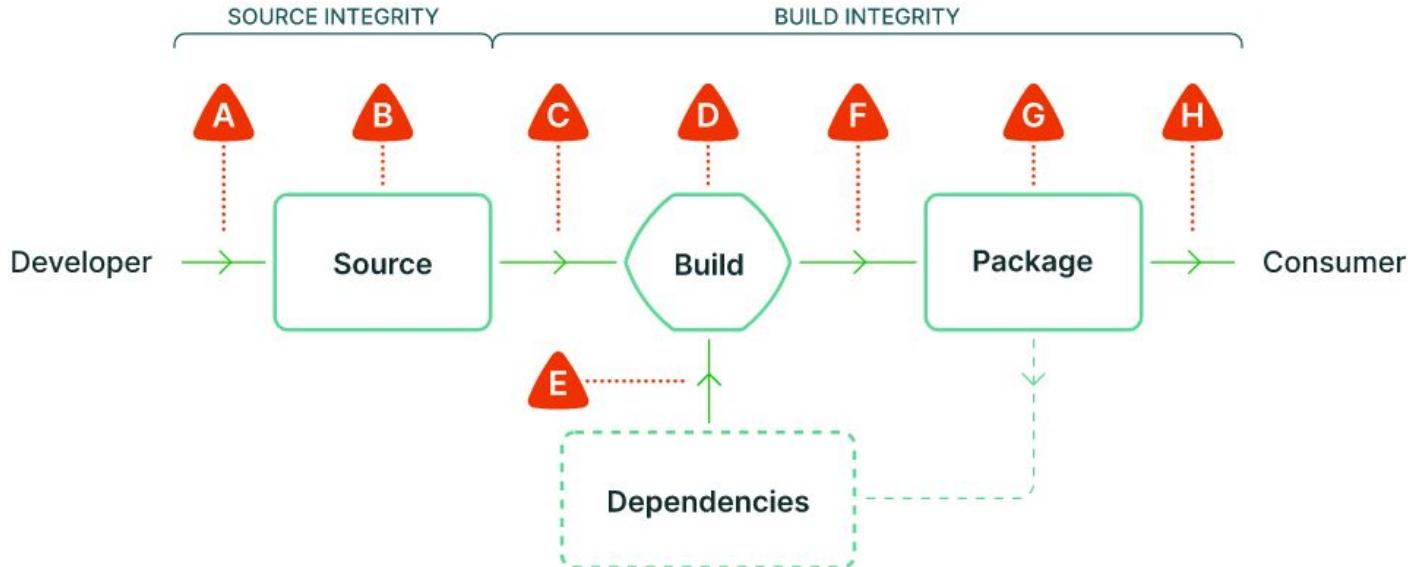
xz Backdoor CVE-2024-3094

One of the most dangerous attacks on the [Linux supply chain](#), mitigated thanks to a lucky break.

How many **backdoors** remain undetected?

Risks in the Software Supply Chain





A Submit unauthorized change
B Compromise source repo

C Build from modified source
D Compromise build process
E Use compromised dependency

F Upload modified package
G Compromise package repo
H Use compromised package



Potential Threats

- Submit unauthorized change (to source repo)
- Compromise source repo
- Build from modified source
- Use compromised dependency
- Compromise build process
- Upload modified package
- Compromise package registry
- Use compromised package

- Dependency becomes unavailable



The JavaScript Supply Chain



“Installing an average npm package introduces an implicit trust on 79 third-party packages and 39 maintainers, creating a surprisingly large attack surface.”

A **massive** ecosystem

npm statistics, 2023 (Sonatype)



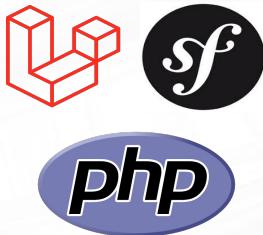
- 2.5M Total Projects
- 37M Total Projects Versions
- 2.6T 2023 Annual Request Volume
- 27% YoY Project Growth
- 18% YoY Download Growth
- 15 Average Versions Released per Project

The PHP Supply Chain



A MODERN PHP APPLICATION

Application

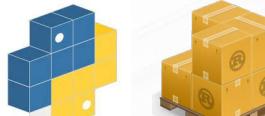


A MODERN PHP APPLICATION

Application



Dependencies

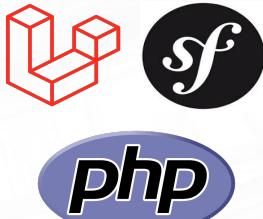


A MODERN PHP APPLICATION

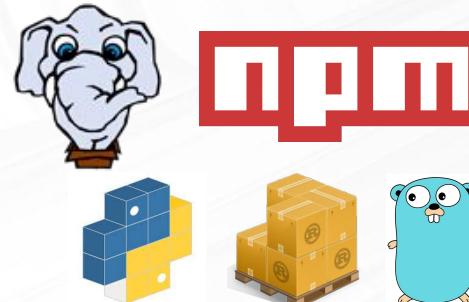
Operating system



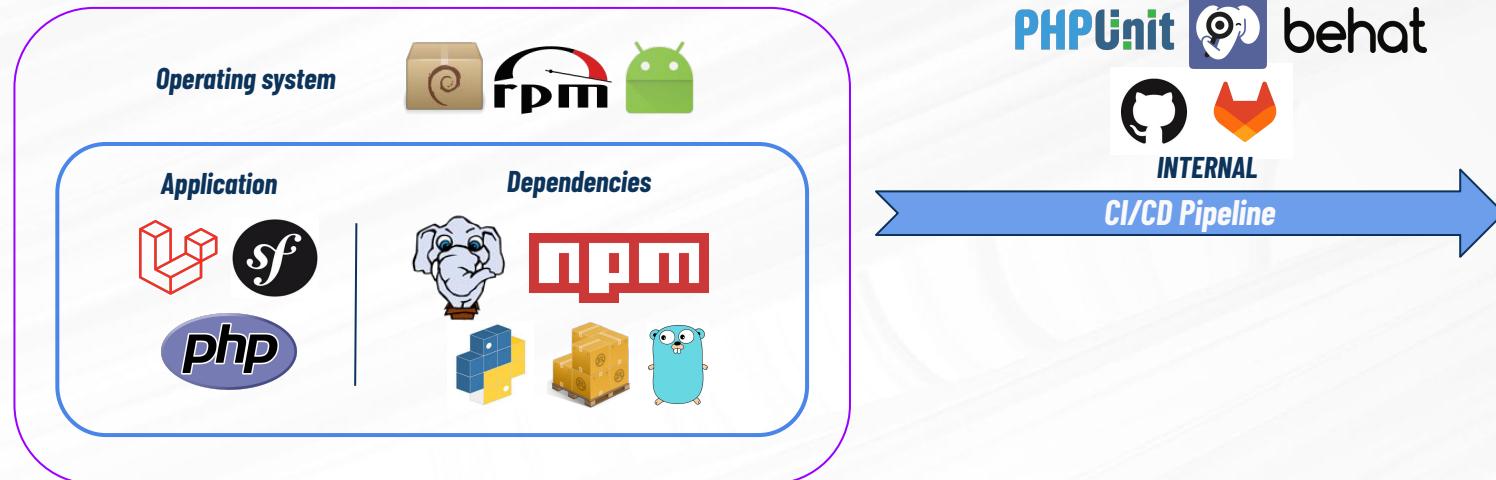
Application



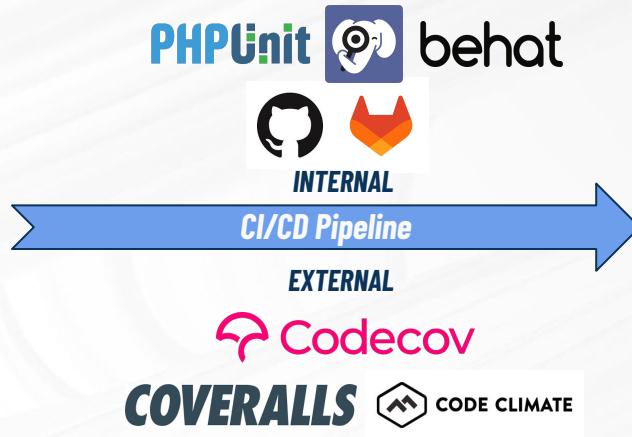
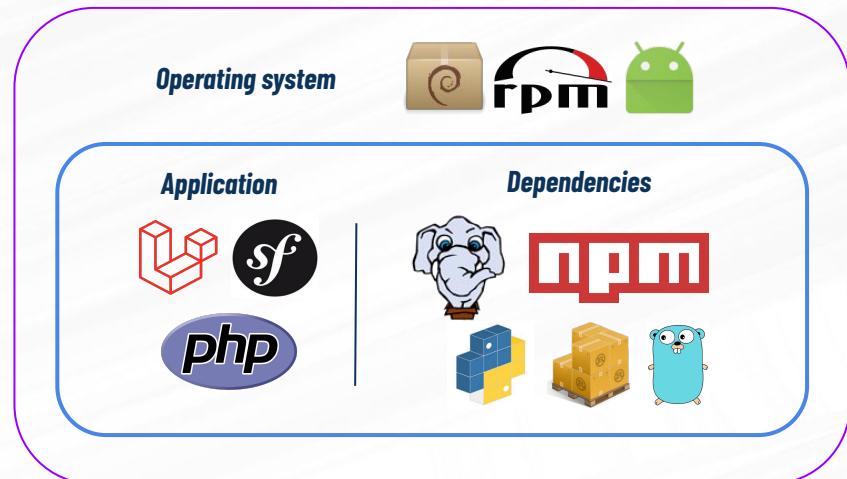
Dependencies



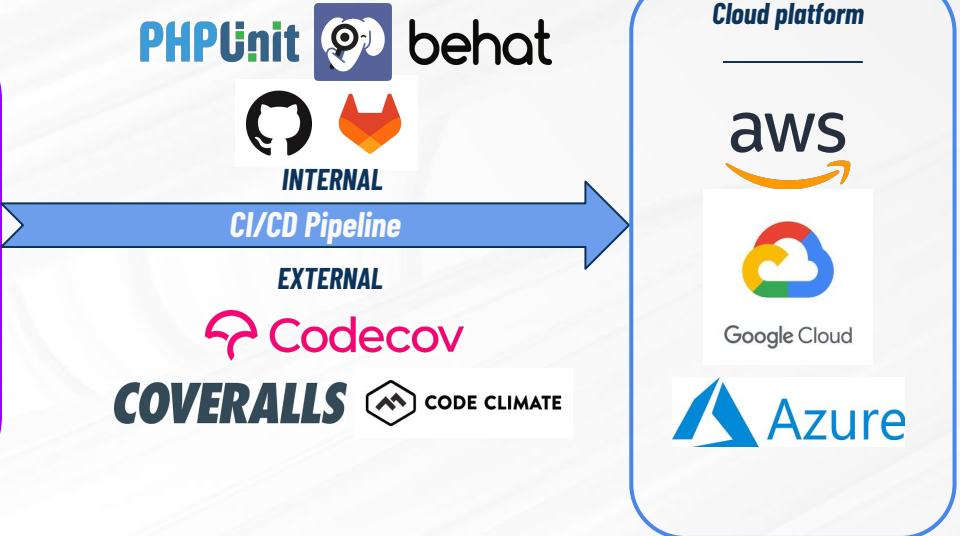
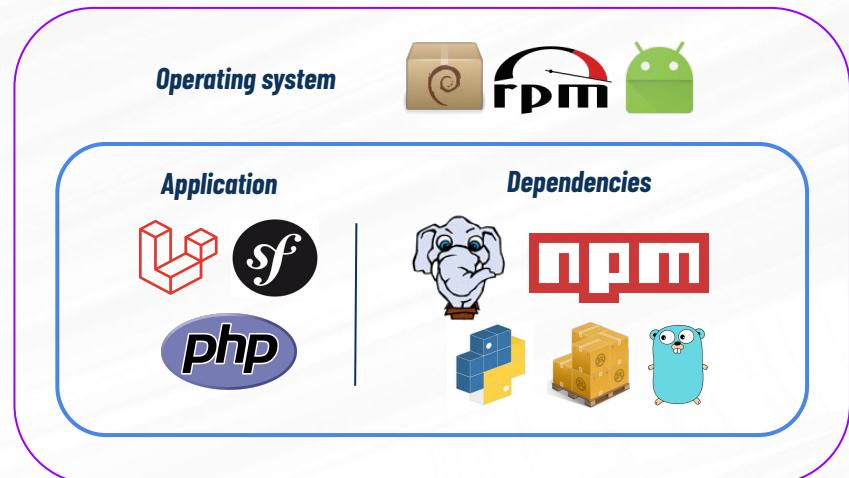
A MODERN PHP APPLICATION



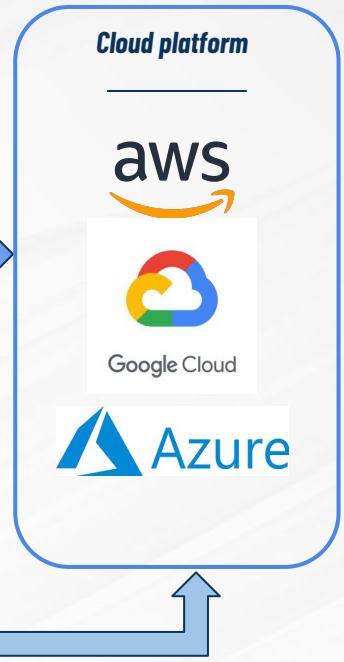
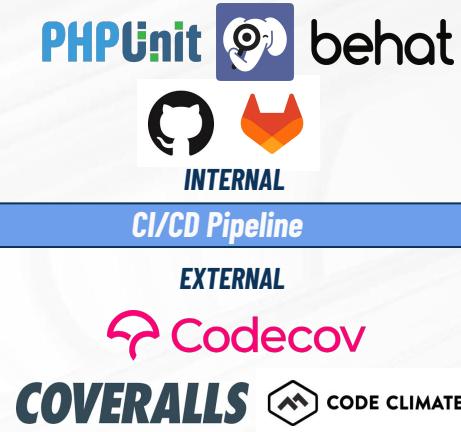
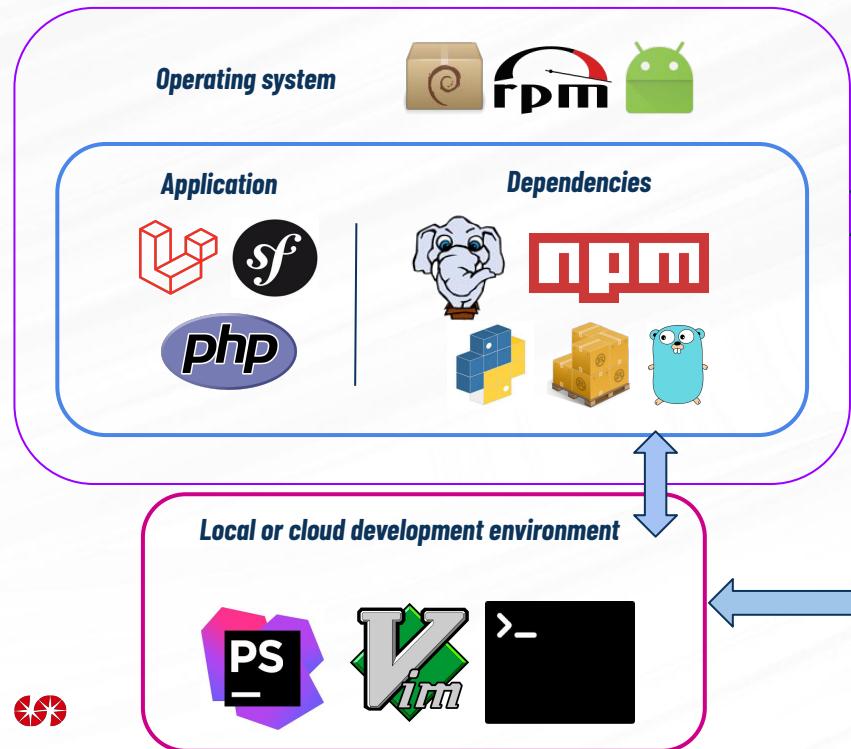
A MODERN PHP APPLICATION



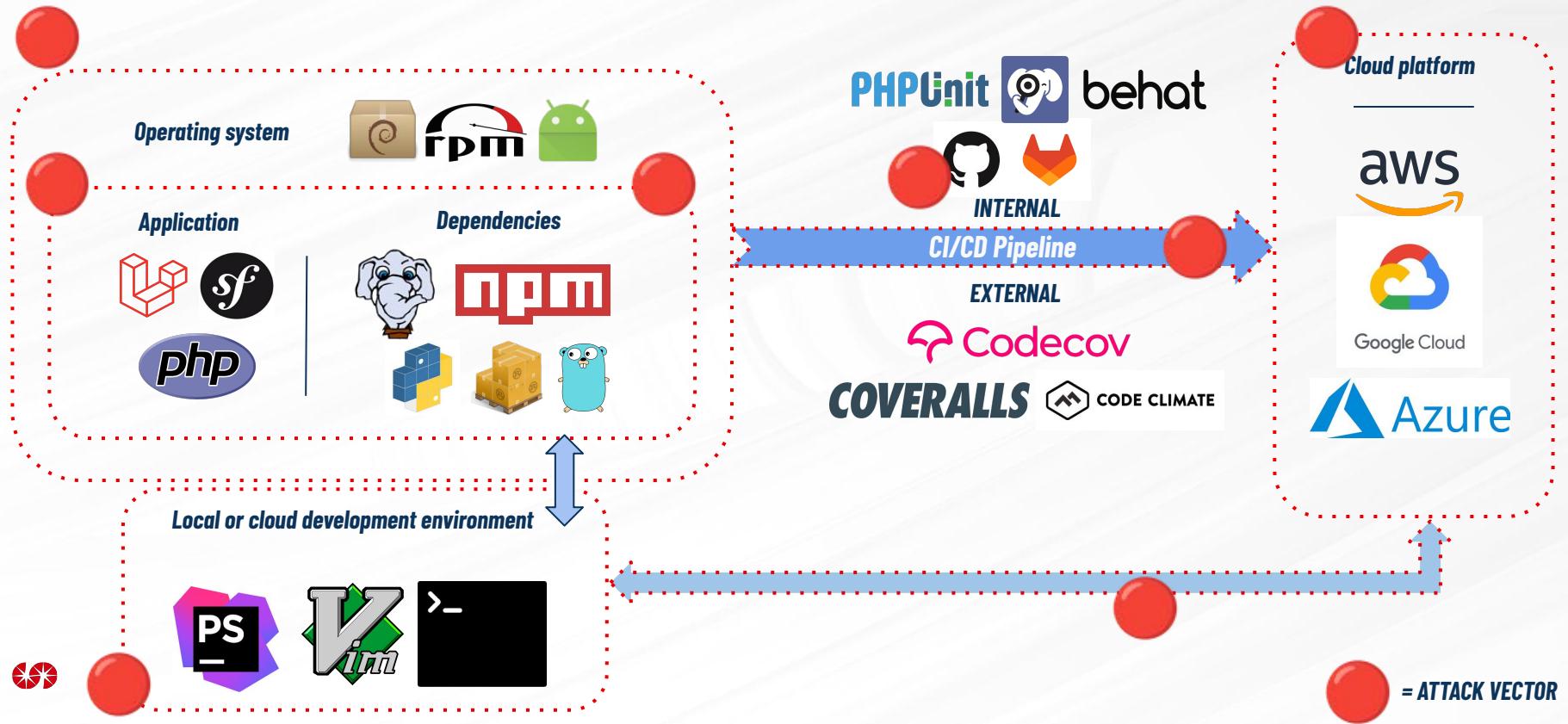
A MODERN PHP APPLICATION



A MODERN PHP APPLICATION

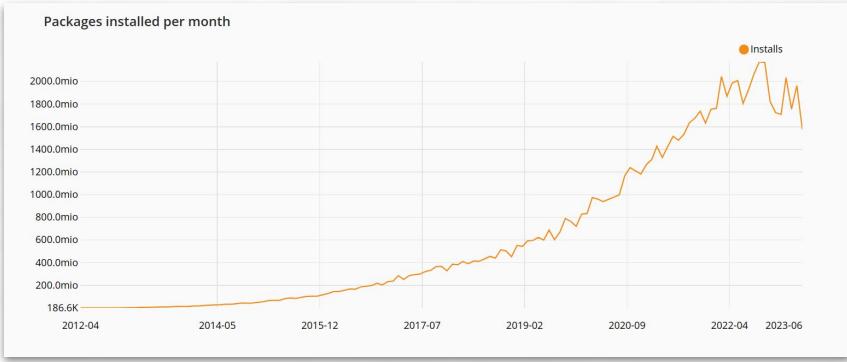
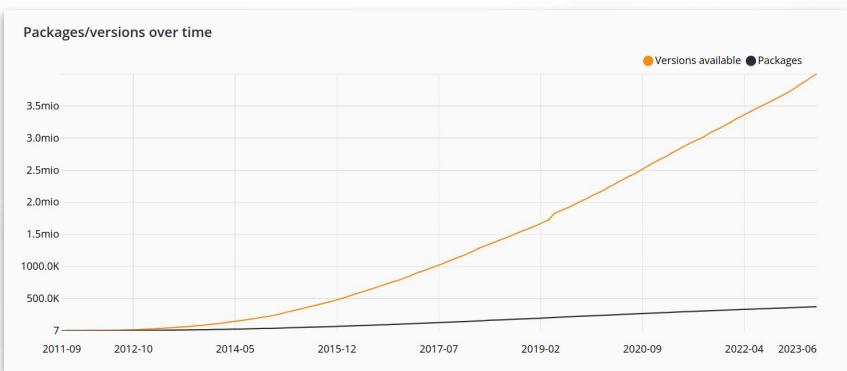


A MODERN PHP APPLICATION



Composer statistics

- Created in 2012 by Nils Adermann and Jordi Boggiano
- The de facto standard for PHP package management
- packagist.org hosts over 300k packages and 2.5M revisions



What is a vulnerability



"A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability."

Common Vulnerabilities and Exposures (CVE) Program



Anything a threat actor can exploit to perform
malicious activity



Dependencies are **crucial**



KNOW YOUR DEPENDENCIES

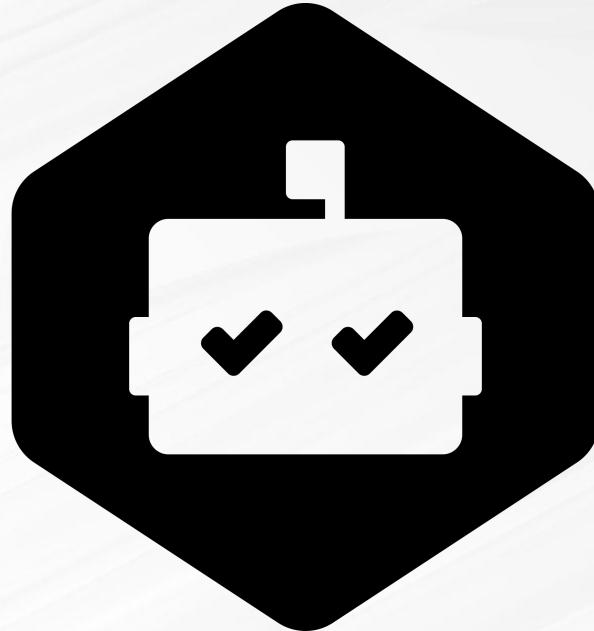


Dependabot



Automated dependency management

- Dependabot is a tool developed independently and then acquired by GitHub to **enhance security and development practices**
- It was developed to automate the process of **updating project dependencies**
- It helps developers to **keep their software up-to-date**
- It's now **fully integrated with GitHub**
- **The core is open source** with MIT License



A screenshot of a GitHub interface showing a list of pull requests. The top navigation bar includes 'Issues', 'Pull requests 13', 'Actions', and a profile icon. A search bar contains the query 'is:pr is:open'. Below the search bar, there are filters for 'Author' and status: '13 Open' and '5 Closed'. The main list displays several pull requests from the 'dependabot' bot, each with a green checkmark icon and a dependency name like 'url-parse', 'follow-redirects', 'ajv', 'tmpl', 'path-parse', and 'merge-deep'. Each PR is labeled as being opened by 'dependabot' and includes a 'dependencies' button. The PRs are ordered by their creation date.

Issues

Pull requests 13

Actions

Pr

is:pr is:open

Author

13 Open ✓ 5 Closed

Bump url-parse from 1.4.7 to 1.5.10 dependencies
#18 opened 11 hours ago by dependabot bot

Bump follow-redirects from 1.10.0 to 1.14.8 dependencies
#16 opened 14 days ago by dependabot bot

Bump ajv from 6.12.0 to 6.12.6 dependencies
#15 opened 14 days ago by dependabot bot

Bump tmpl from 1.0.4 to 1.0.5 dependencies
#12 opened on Sep 22, 2021 by dependabot bot

Bump path-parse from 1.0.6 to 1.0.7 dependencies
#11 opened on Aug 12, 2021 by dependabot bot

Bump merge-deep from 3.0.2 to 3.0.3 dependencies

OO HACKINBO Spring 2021 Edition 22/12/2021

How does Dependabot work

- **Scans repositories** for outdated or insecure dependencies
- **Opens pull requests** to update dependencies to the latest version
- Can be configured to **run at specified intervals**
- **Provides alerts** for vulnerabilities found in current dependencies
- Support **private** and **public** repositories on GitHub
- Can be integrated with other SCM like **GitLab**

The screenshot shows a GitHub repository page for 'erinhav / havens-favourites'. The 'Security' tab is selected, displaying 245 Dependabot alerts. A search bar at the top right contains the query 'is:open'. The alerts are listed in a table with columns for Package, Ecosystem, Manifest, and Sort. Most alerts are critical or moderate severity, related to Pillow and tensorflow packages.

Package	Ecosystem	Manifest	Sort
Pillow (pip)	requirements.txt	#245	Critical
Pillow (pip)	requirements.txt	#244	Critical
Pillow (pip)	requirements.txt	#243	Critical
tensorflow (pip)	requirements.txt	#242	Moderate
tensorflow (pip)	requirements.txt	#241	Moderate
tensorflow (pip)	requirements.txt	#240	Moderate
tensorflow (pip)	requirements.txt	#239	Moderate
tensorflow (pip)	requirements.txt	#238	Moderate

erinhav / havens-favourites

Search or jump to... Unwatch 1 Fork 0 Star 0

erinhav / havens-favourites Private

Code Issues Pull requests 4 Actions Projects Wiki Security Insights Settings

Overview Security policy Security advisories Dependabot alerts

Dismiss all

is:open package:lodash

Clear current search query, filters, and sorts

7 Open 0 Closed

Package Ecosystem Manifest Sort

Command Injection in lodash High
lodash (npm) · package-lock.json · #13 opened 7 minutes ago

Regular Expression Denial of Service (ReDoS) in lodash Moderate
lodash (npm) · package-lock.json · #12 opened 7 minutes ago

Prototype Pollution in lodash High
lodash (npm) · package-lock.json · #8 opened 7 minutes ago

Prototype pollution in lodash Moderate
lodash (npm) · package-lock.json · #6 opened 7 minutes ago

Prototype Pollution in lodash Critical
lodash (npm) · package-lock.json · #5 opened 7 minutes ago

Prototype Pollution in lodash High
lodash (npm) · package-lock.json · #3 opened 7 minutes ago

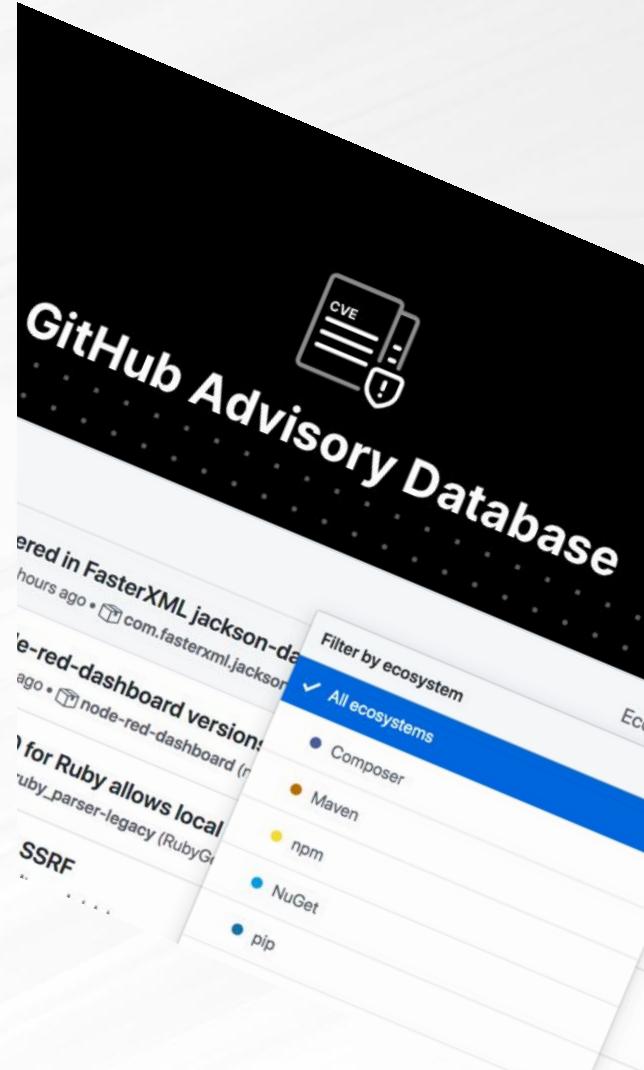
Prototype Pollution in lodash Low
lodash (npm) · package-lock.json · #2 opened 7 minutes ago

Where is the **vulnerabilities** information coming from



GitHub Advisory Database

- Dependabot alerts are powered by the GitHub Advisory Database
<https://github.com/advisories>
- This is the **largest vulnerability database** available worldwide
- It's maintained by a **dedicated team of curators** and supported by community contributions
- Security advisories are published as JSON files in the **Open Source Vulnerability (OSV)** format
- The GitHub Security Advisories monitor several sources for vulnerabilities, the most prominent of which is the **National Vulnerability Database (NVD)**



National Vulnerability Database



- The NVD is the **US government repository** for vulnerability management data
- It represents this data using the **Security Content Automation Protocol (SCAP)**
- It's managed by the US government agency the **National Institute of Standards and Technology**
- All vulnerabilities are assigned a **Common Vulnerabilities and Exposures (CVE)** identifier
- It scores vulnerabilities using the **Common Vulnerability Scoring System (CVSS)**

CVE identifiers

- The **CVE Program** was launched in 1999
- The primary purpose is to **uniquely identify vulnerabilities**
- A publicly disclosed security issue is assigned a **CVE ID number**
- CVE associates **specific versions** of a software or library to the vulnerability
- Using CVEs ensures **consistent referencing** and sharing of information



**Common
Vulnerabilities &
Exposures**



Are there **other** databases?



A distributed vulnerability database for Open Source

An open, precise, and distributed approach to producing and consuming vulnerability information for open source.

[Search Vulnerability Database](#)[Use the API](#)[Vulnerability Scanner](#)[Remediation Tools](#)[GitHub Workflows](#)

Ecosystems



AlmaLinux 3450 Alpine 890 Android 3996 Bitnami 1365 crates.io 9906 Debian 30062 GIT 2210 Go 13573 Linux 4905 Maven 14617 npm 591 NuGet 3322 OSS-Fuzz 3763 Packagist 12062 PyPI 1192 Rocky Linux 794 RubyGems 31 SwiftURL 5183 Ubuntu



Open Source Vulnerability DB

- OSV was **launched in 2004**
- OSV is an **open and distributed approach** to producing and consuming vulnerability information for Open Source Software
- **OSV Schema** introduced in 2021 is a **data format** to describe vulnerabilities that map to precise version
- OSV Schema **created by members of OpenSSF** and hosted by the foundation
- OSV serves as **aggregator of vulnerability db** that have adopted the schema, including GitHub Advisory, PyPA, RustSec etc...



Scanning vulnerabilities with **different tools**



```

> ✓ Pull ghcr.io/google/osv-scanner-action:v1.6.1                                2s
> ✓ Run actions/checkout@b4ffde65f46336ab88eb53be808477a3936bae11                  1s
> ✓ Checkout target branch                                                       0s
> ✓ Run scanner on existing code                                                 10s
> ✓ Checkout current branch                                                       0s
> ✓ Run scanner on new code                                                       10s
> ✘ Run osv-scanner-reporter                                                    0s
1 ➤ Run google/osv-scanner-action/osv-reporter-action@staging
8 /usr/bin/docker run --name ghcriogoogleosvscanneractionv161_b77d91 --label 06b4cd --workdir /github/workspace
--rm -e "INPUT_SCAN_ARGS" -e "HOME" -e "GITHUB_JOB" -e "GITHUB_REF" -e "GITHUB_SHA" -e "GITHUB_REPOSITORY" -e
"GITHUB_REPOSITORY_OWNER" -e "GITHUB_REPOSITORY_ID" -e "GITHUB_RUN_ID" -e "GITHUB_RUN_NUMBER" -e
"GITHUB_RETENTION_DAYS" -e "GITHUB_RUN_ATTEMPT" -e "GITHUB_REPOSITORY_ID" -e "GITHUB_ACTOR_ID" -e
"GITHUB_ACTOR" -e "GITHUB_TRIGGERING_ACTOR" -e "GITHUB_WORKFLOW" -e "GITHUB_HEAD_REF" -e "GITHUB_BASE_REF" -e
"GITHUB_EVENT_NAME" -e "GITHUB_SERVER_URL" -e "GITHUB_API_URL" -e "GITHUB_GRAPHQL_URL" -e "GITHUB_REF_NAME" -e
"GITHUB_REF_PROTECTED" -e "GITHUB_REF_TYPE" -e "GITHUB_WORKFLOW_REF" -e "GITHUB_WORKFLOW_SHA" -e
"GITHUB_WORKSPACE" -e "GITHUB_ACTION" -e "GITHUB_EVENT_PATH" -e "GITHUB_ACTION_REPOSITORY" -e
"GITHUB_ACTION_REF" -e "GITHUB_PATH" -e "GITHUB_ENV" -e "GITHUB_STEP_SUMMARY" -e "GITHUB_STATE" -e
"GITHUB_OUTPUT" -e "RUNNER_OS" -e "RUNNER_ARCH" -e "RUNNER_NAME" -e "RUNNER_ENVIRONMENT" -e
"RUNNER_TOOL_CACHE" -e "RUNNER_TEMP" -e "RUNNER_WORKSPACE" -e "ACTIONS_RUNTIME_URL" -e "ACTIONS_RUNTIME_TOKEN"
-e "ACTIONS_CACHE_URL" -e "ACTIONS_RESULTS_URL" -e GITHUB_ACTIONS=true -e CI=true --entrypoint "/root/osv-
reporter" -v "/var/run/docker.sock":"/var/run/docker.sock" -v
"/home/runner/work/_temp/_github_home":"/github/home" -v
"/home/runner/work/_temp/_github_workflow":"/github/workflow" -v
"/home/runner/work/_temp/_runner_file_commands":":"/github/file_commands" -v
"/home/runner/work/osv.dev/osv.dev":"/github/workspace" ghcr.io/google/osv-scanner-action:v1.6.1 ...
output=results.sarif
9 --old=old-results.json
10 --new=new-results.json
11 --gh-annotations=true
12 --fail-on-vuln=true"
13 +-----+-----+-----+-----+-----+
14 | OSV URL | CVSS | ECOSYSTEM | PACKAGE | VERSION | SOURCE |
15 +-----+-----+-----+-----+-----+
16 | https://osv.dev/G0-2023-2192 | Go | stdlib | 1.21.1 | tools/datastore-remover/go.mod |
17 | https://osv.dev/G0-2023-2185 | Go | stdlib | 1.21.1 | tools/datastore-remover/go.mod |
18 | https://osv.dev/G0-2023-2186 | Go | stdlib | 1.21.1 | tools/datastore-remover/go.mod |
19 | https://osv.dev/G0-2023-2382 | Go | stdlib | 1.21.1 | tools/datastore-remover/go.mod |
20 +-----+-----+-----+-----+-----+
21 Error: tools/datastore-remover/go.mod
22 +-----+-----+-----+
23 | PACKAGE | VULNERABILITY ID | CVSS | CURRENT VERSION | FIXED VERSION |
24 +-----+-----+-----+

```

OSV-Scanner

- Tool written in Go that **scans the project dependencies** to link them with known vulnerabilities
- Frontend to the **OSV database**
- **Analyses all transitive dependencies**, manifests, SBOMs and commit hashes
- OSV-Scanner is integrated into **OpenSSF Scorecard**

Renovate

- Multi-platform automatic dependency updates
- Dependabot competitor
- Customizable via config file
- Supports many different SCM
- Can be self-hosted
- Open Source with AGPL





Snyk Open Source

- Snyk Open Source is a vulnerability scanner part of the Snyk Platform
- Snyk is a member of OpenSSF
- It also scans for licensing issues
- Can be integrated in any step of the SDLC
- Uses the Snyk Vulnerability Database
- Can automatically fix vulnerabilities from the command-line, code editor or CI/CD pipeline

Best practices for vulnerability scanning



What to look for in an open source security tool

- **Comprehensive view** of packages and vulnerabilities affecting them
 - ◆ Are you depending on vulnerable components?
- **Automation**
 - ◆ Set policies around fixes, pull requests, patches, and upgrades
- **Integrations** with developer tools, workflows, and pipelines
 - ◆ Developers should easily see and apply fixes
- **Up-to-date and enriched database** that goes beyond known CVEs
 - ◆ Look beyond public databases for proprietary, curated databases
- **Continuous monitoring** of projects
 - ◆ Applications should monitor themselves and be equipped to defend themselves against attacks



How can you contribute?



Ways to Participate



[Join the OpenSSF Mailing List](#)



[Follow us on LinkedIn](#)



[Follow us on Mastodon](#)



[Follow us on Facebook](#)



[Subscribe to our YouTube Channel](#)



[Follow us on X](#)



[Join a Working Group/Project](#)



[Access the Public Meetings Calendar](#)



[Participate on Slack](#)



[Follow OpenSSF on GitHub](#)



[Become an Organizational Member](#)



Attend a Public Meeting

bit.ly/ossf-calendar



general

✓ Joined · 2,026 members · This channel is for workspace-wide communication and announcements. All memb...

wg_security_tooling

526 members · This WG is chaired by [@Josh Bressers](#)

wg_supply_chain_integrity

517 members · Our objective is to enable open source maintainers, contributors and end-users to understand an...

wg_securing_critical_projects

✓ Joined · 460 members · Helping allocate resources to secure the critical open source projects we all depend ...

slsa

✓ Joined · 451 members · discuss slsa framework

wg_best_practices_ossdev

428 members · The Best Practices for OSS Developers working group is dedicated to raising awareness and educ...

wg_vulnerability_disclosures

427 members · OpenSSF Vulnerability Disclosures Working Group seeks to help improve the overall security of t...

security_scorecards

397 members · security scorecard project <https://github.com/ossf/scorecard> Bi-Weekly meetings on Thursday 1:...

Message on Slack

slack.openssf.org



Follow us on Social Media



[X](#)
[@openssf](#)



[LinkedIn](#)
OpenSSF



[Mastodon](#)
[social.lfx.dev/
@openssf](https://social.lfx.dev/@openssf)



[YouTube](#)
OpenSSF



[Facebook](#)
OpenSSF

Thank you.



Edoardo Dusi

Developer Relations Engineer @ SparkFabrik

edoardo.dusi@sparkfabrik.com

@edodus

[@edo@continuousdelivery.social](mailto:edo@continuousdelivery.social)

