

Building a better database

How GitHub Structures their Advisory Database to Drive Developer Outcomes

@darakian - 25th March 2024

Who am I?

Hi, I'm Jon (aka Darakian) 🙋



- GitHub since 2021
- Security since 2018
- Tech since 2008
- Nerd since time immemorial
- <https://github.com/darakian/>

We are the GitHub Security lab

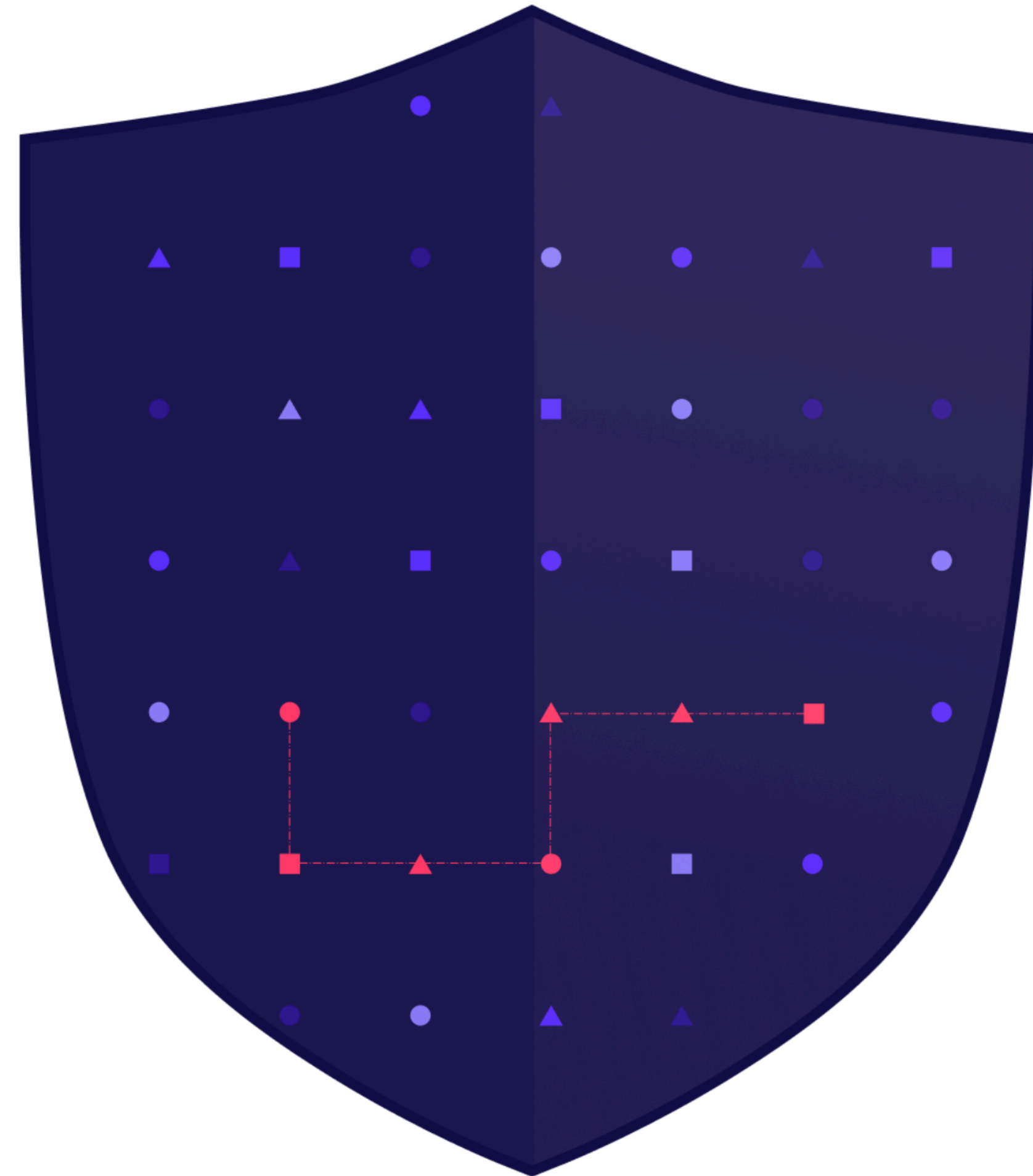
We want to secure your software

GitHub Security Lab

Securing the world's software, together

GitHub Security Lab's mission is to inspire and enable the community to secure the open source software we all depend on.

Follow @GHSecurityLab



What do I do?

I'm a librarian 

- I curate advisories for the advisory database
- Ensure correctness, completeness and conciseness
- Quality over quantity
- <https://github.com/advisories>
- <https://github.com/github/advisory-database>



GitHub Advisory Database

Security vulnerability database inclusive of CVEs and GitHub originated security advisories from the world of open source software.

GitHub reviewed advisories

All reviewed	14,490
Composer	2,242
Erlang	22
GitHub Actions	11
Go	1,214
Maven	3,951
npm	3,147
NuGet	510
pip	2,083
Pub	7
RubyGems	743
Rust	657
Swift	29

Unreviewed advisories

All unreviewed	197,394
----------------	---------

CC-BY-4.0 License

Language support ⓘ

About GitHub Advisory Database

Search by CVE/GHSA ID, package, severity, ecosystem, credit...

14,490 advisories Severity CWE Sort

- Improper Control of Generation of Code ('Code Injection') in jai-ext** **Critical**
CVE-2022-24816 was published for it.geosolutions.jaiext.jiffle:jt-jiffle (Maven) 1 hour ago
- Pow Mnesia cache doesn't invalidate all expired keys on startup** **Moderate**
CVE-2023-42446 was published for pow (Erlang) 4 hours ago
- A remote command execution (RCE) vulnerability in the /api/runscript endpoint of FUXA** **High**
CVE-2023-33831 was published for @frangoteam/fuxa (npm) yesterday
- Vyper has incorrect re-entrancy lock when key is empty string** **Moderate**
CVE-2023-42441 was published for vyper (pip) yesterday
- Arbitrary File Overwrite in Eclipse JGit** **High**
CVE-2023-4759 was published for org.eclipse.jgit:org.eclipse.jgit (Maven) yesterday
- Cross-Site Request Forgery (CSRF) in usememos/memos** **High**
CVE-2023-5036 was published for github.com/usememos/memos (Go) 2 days ago
- Directus affected by VM2 sandbox escape vulnerability** **High**
GHSA-22rr-f3p8-5gf8 was published for directus (npm) 4 days ago
- Jetty's OpenId Revoked authentication allows one request** **Low**
CVE-2023-41900 was published for org.eclipse.jetty:jetty-openid (Maven) 4 days ago
- LibreNMS Cross-site Scripting vulnerability** **Critical**
CVE-2023-4982 was published for librengms/librenms (Composer) 5 days ago
- LibreNMS Cross-site Scripting vulnerability** **High**
CVE-2023-4981 was published for librengms/librenms (Composer) 5 days ago

First and foremost what are we doing here?

Fixing code!

- People don't want to ship vulnerable code
- People don't want their time wasted by fuzzy matching
- People do understand that vulns are nuanced
- People do appreciate a best effort job when the effort is obvious
- People will forgive you for (understandable) mistakes

First and foremost what are we doing here?

What are good outcomes?

- Minimize time from public disclosure to code fix deployed
- Minimize false positives to save developer time
- Maximize utility per advisory
- Maximize human curation impact
- Avoid the tar pit

The developer perspective

NVD Dashboard

2023-07-18

CVEs Received and Processed

Time Period	New CVEs Received by NVD	New CVEs Analyzed by NVD	Modified CVEs Received by NVD	Modified CVEs Re-analyzed by NVD
Today	171	156	15	0

CVSS V3 Score Distribution



Severity	Number of Vulns
CRITICAL	20138
HIGH	54575

but which ones do I care about?



Surely not all of them

Total	220655	CVE vulnerabilities	220655
Received	1	Checklists	617
Awaiting Analysis	574	US-CERT Alerts	249
Undergoing Analysis	607	US-CERT Vuln Notes	4486
Modified	73565	OVAL Queries	10286
Deferred	115	CPE Names	1112465
Rejected	12805		



HIGH	56835
MEDIUM	104175
LOW	19076

Scope

We can do anything so long as we don't do everything

Supported ecosystems

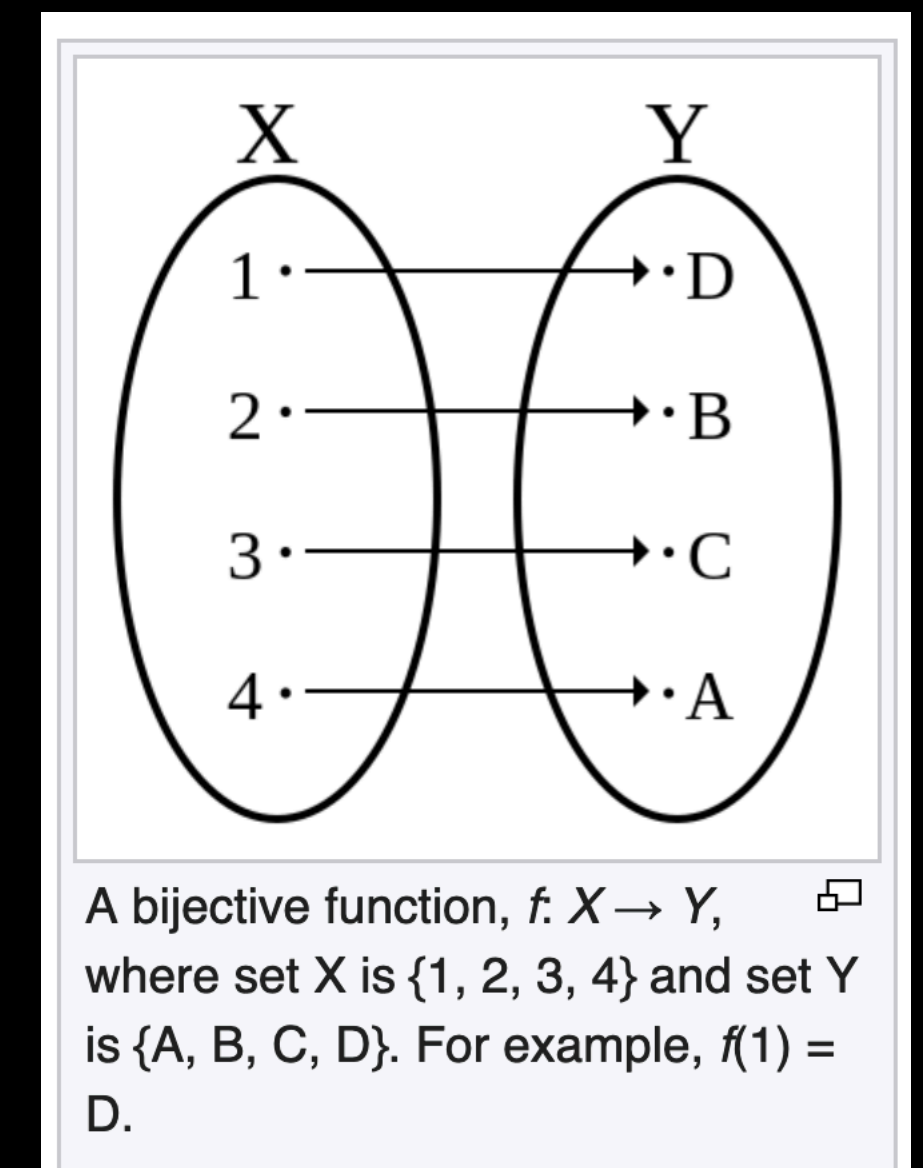
Unfortunately, we cannot accept community contributions to advisories outside of our supported ecosystems. Our curation team reviews each community contribution thoroughly and needs to be able to assess each change.

Generally speaking, our ecosystems are the namespace used by a package registry. As such they're focused on packages within the registry which tend to be dependencies used in software development.

Our supported ecosystems are:

- Composer (registry: <https://packagist.org>)
- Erlang (registry: <https://hex.pm/>)
- GitHub Actions (registry: <https://github.com/marketplace?type=actions>)
- Go (registry: <https://pkg.go.dev/>)
- Maven (registry: <https://repo.maven.apache.org/maven2>)
- npm (registry: <https://www.npmjs.com/>)
- NuGet (registry: <https://www.nuget.org/>)
- pip (registry: <https://pypi.org/>)
- Pub (registry: <https://pub.dev/>)
- RubyGems (registry: <https://rubygems.org/>)
- Rust (registry: <https://crates.io/>)
- Swift (registry: [namespaced by dns](#))

If you have a suggestion for a new ecosystem we should support, please open an [issue](#) for discussion.



(Ecosystem, Package Name) \Rightarrow one and ONLY one thing

(Ecosystem, Package Name) \Leftarrow one and ONLY one thing

Scope

We can do anything so long as we don't do everything

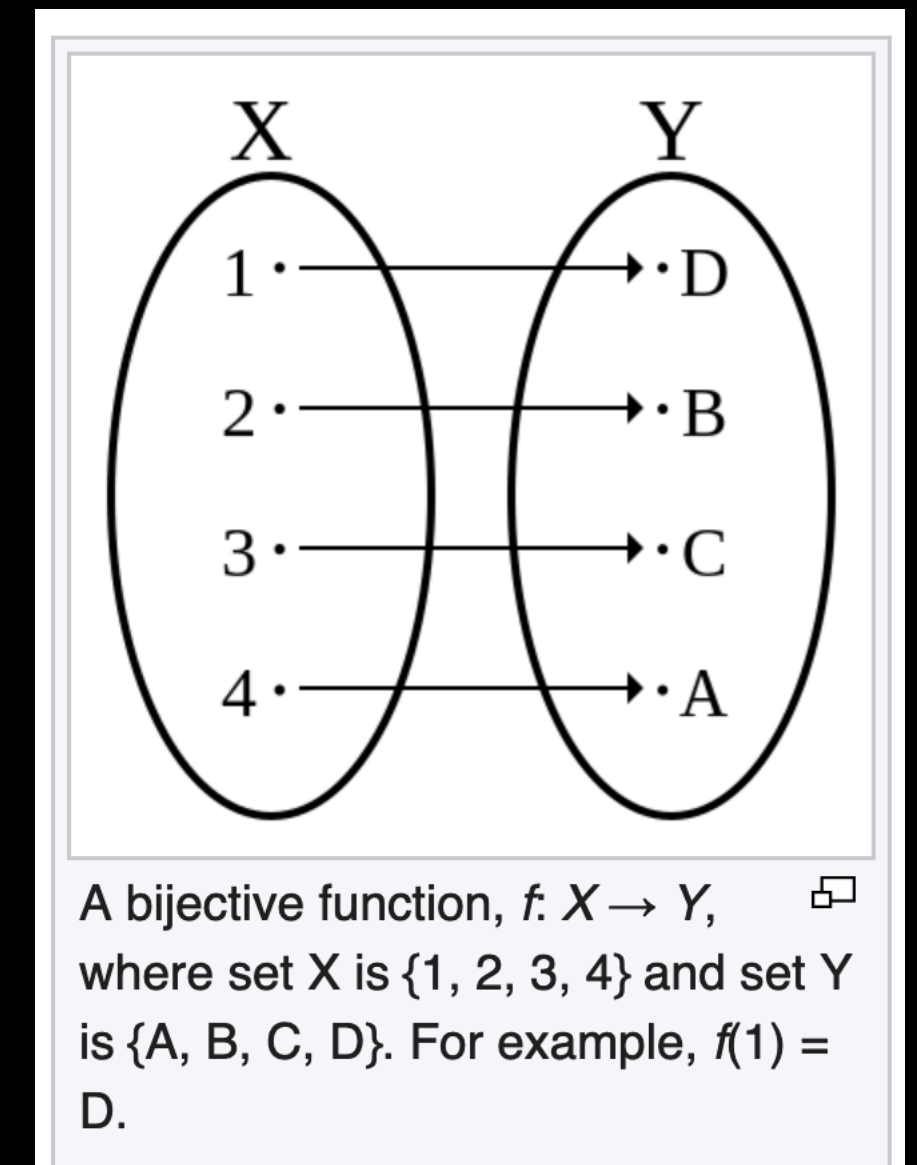
Supported ecosystems

Unfortunately, we cannot accept community contributions to advisories outside of our supported ecosystems. Our curation team reviews each community contribution thoroughly and needs to be able to assess each change.

Generally speaking, our ecosystems are the namespace used by a package registry. As such they're focused on packages within the registry which tend to be dependencies used in software development.

Our supported ecosystems are:

- Composer (registry: <https://packagist.org>)
- Erlang (registry: <https://hex.pm/>)
- GitHub Actions (registry: <https://github.com/marketplace?type=actions>)
- Go (registry: <https://pkg.go.dev/>)
- Maven (registry: <https://repo.maven.apache.org/maven2>)
- npm (registry: <https://www.npmjs.com/>)
- NuGet (registry: <https://www.nuget.org/>)
- pip (registry: <https://pypi.org/>)
- Pub (registry: <https://pub.dev/>)
- RubyGems (registry: <https://rubygems.org/>)
- Rust (registry: <https://crates.io/>)
- Swift (registry: [namespaced by dns](#))



(Ecosystem, Package Name) => one and ONLY one thing

(Ecosystem, Package Name) <= one and ONLY one thing


If you have a suggestion for a new ecosystem we should support, please open an [issue](#) for discussion.

CPE is not bijective

Four different roots

Known Affected Software Configurations [Switch to CPE 2.2](#)


Configuration 1 ([hide](#))

 cpe:2.3:a:lodash:lodash:*:*:*:*:node.js:*:*	Up to (excluding)
Show Matching CPE(s)	4.17.5

<https://nvd.nist.gov/vuln/detail/CVE-2018-3721>

Known Affected Software Configurations [Switch to CPE 2.2](#)




Configuration 1 ([hide](#))

 cpe:2.3:a:nodejs:undici:*:*:*:*:node.js:*:*	Up to (excluding)
Show Matching CPE(s)	5.26.2

<https://nvd.nist.gov/vuln/detail/CVE-2023-45143>

Known Affected Software Configurations [Switch to CPE 2.2](#)


Configuration 1 ([hide](#))

 cpe:2.3:a:npmjs:semver:*:*:*:*:node.js:*:*	Up to (excluding)	
Show Matching CPE(s)	5.7.2	
 cpe:2.3:a:npmjs:semver:*:*:*:*:node.js:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	6.0.0	6.3.1
 cpe:2.3:a:npmjs:semver:*:*:*:*:node.js:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	7.0.0	7.5.2

<https://nvd.nist.gov/vuln/detail/CVE-2022-25883>

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 ([hide](#))

 cpe:2.3:a:mathjs_project:mathjs:*:*:*:*:*:*	Up to (excluding)
Show Matching CPE(s)	3.17.0

<https://nvd.nist.gov/vuln/detail/CVE-2017-1001003>

CPE is not bijective

Index for the benefit of the scanner

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 ([hide](#))

✖ cpe:2.3:a:lodash:lodash:*:*:*:*:node.js:**

[Show Matching CPE\(s\)](#)

Package

 **lodash** (npm)

Affected versions

< 4.17.5

Patched versions

4.17.5

<https://github.com/advisories/GHSA-fvqr-27wr-82fm>

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 ([hide](#))

✖ cpe:2.3:a:nodejs:undici:*:*:*:*:node.js:**

[Show Matching CPE\(s\)](#)

Package

 **undici** (npm)

Affected versions

< 5.26.2

Patched versions

5.26.2

<https://github.com/advisories/GHSA-wqq4-5wpv-mx2g>

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 ([hide](#))

✖ cpe:2.3:a:npmjs:semver:*:*:*:*:node.js:**

[Show Matching CPE\(s\)](#)

Up to (excluding)

5.7.2

✖ cpe:2.3:a:npmjs:semver:*:*:*:*:node.js:**

[Show Matching CPE\(s\)](#)

From (including)

6.0.0

✖ cpe:2.3:a:npmjs:semver:*:*:*:*:node.js:**

[Show Matching CPE\(s\)](#)

From (including)

7.0.0

Package

 **semver** (npm)

Affected versions

>= 7.0.0, < 7.5.2

Patched versions

7.5.2

>= 6.0.0, < 6.3.1

6.3.1

< 5.7.2

5.7.2

<https://github.com/advisories/GHSA-c2qf-rxjj-qggw>

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 ([hide](#))

✖ cpe:2.3:a:mathjs_project:mathjs:*:*:*:*:*

[Show Matching CPE\(s\)](#)

Package

 **mathjs** (npm)

Affected versions

< 3.17.0

Patched versions

3.17.0

<https://github.com/advisories/GHSA-pv8x-p9hq-j328>

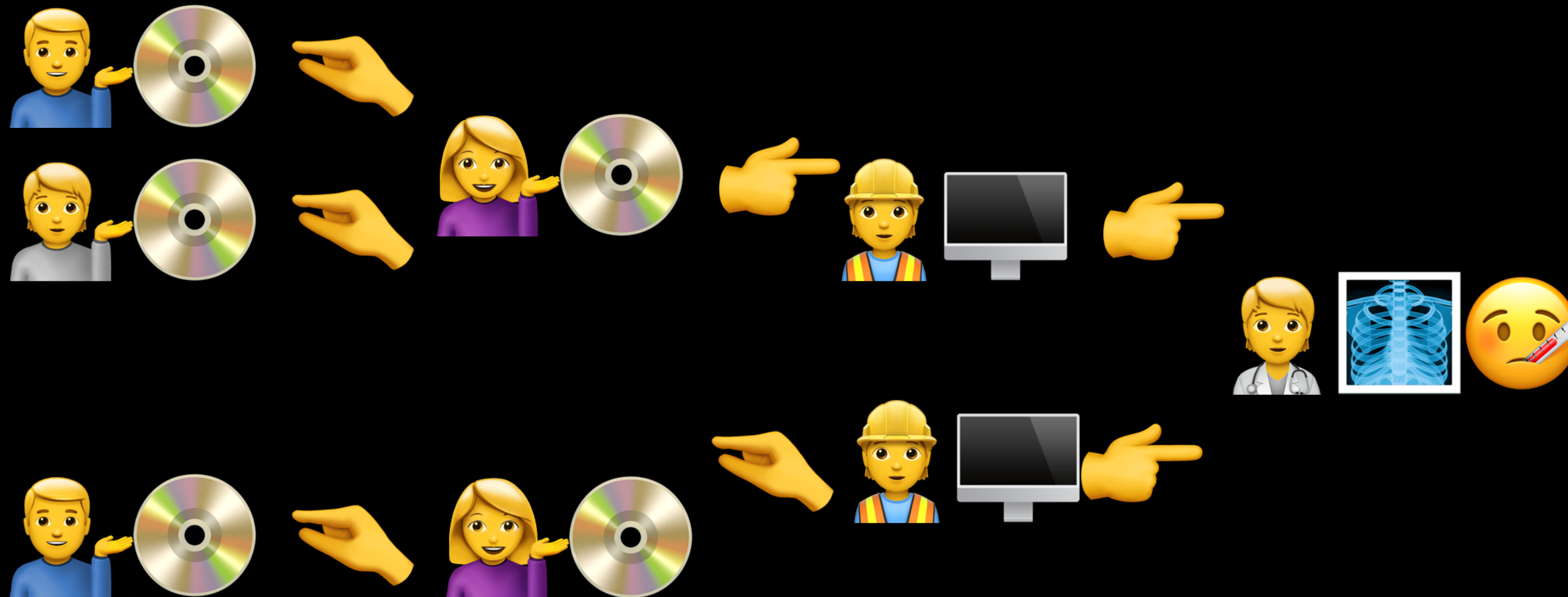
Anatomy of an attack

A chain of supply



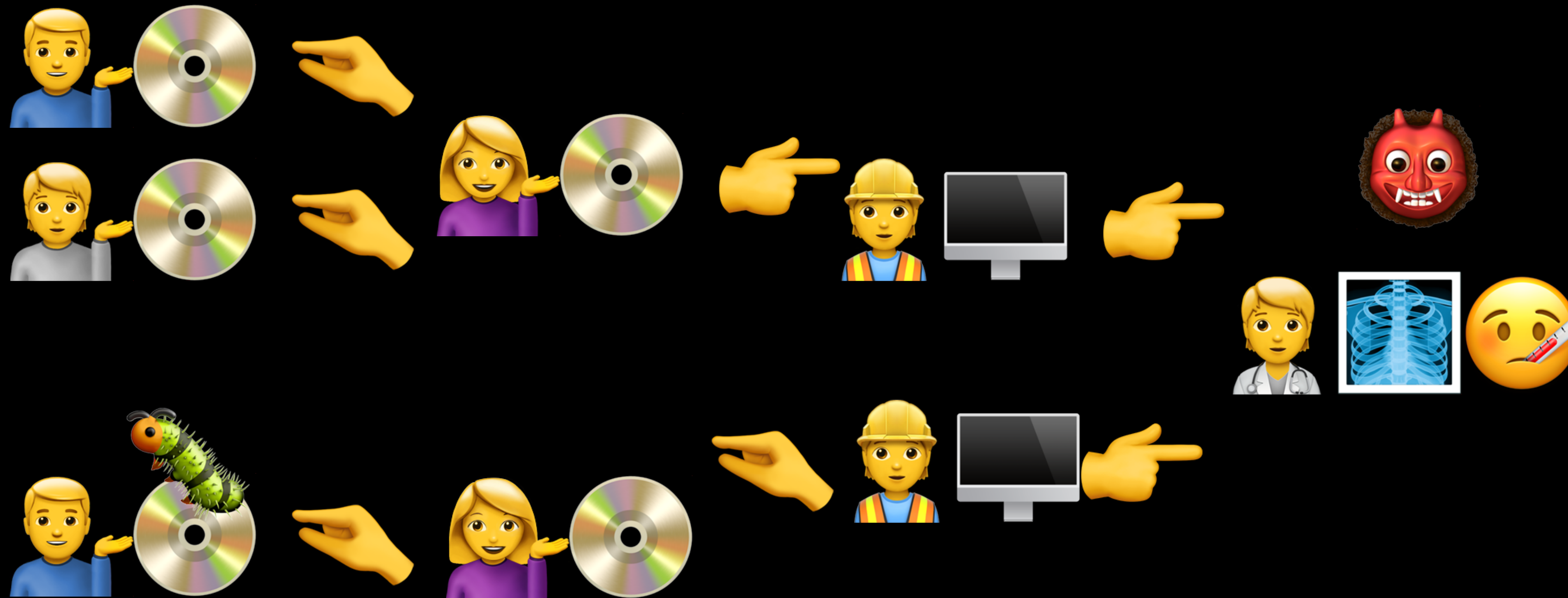
Anatomy of an attack

A web of supply



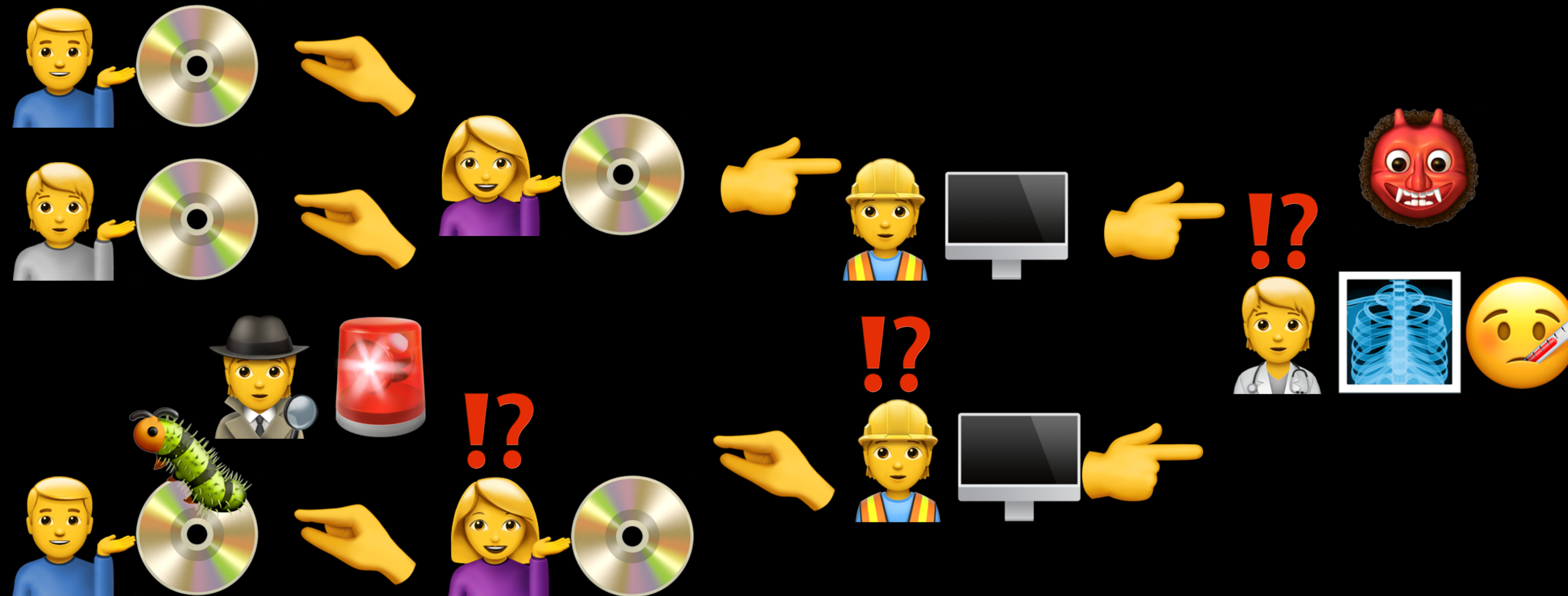
Anatomy of an attack

Where bugs manifest in the web



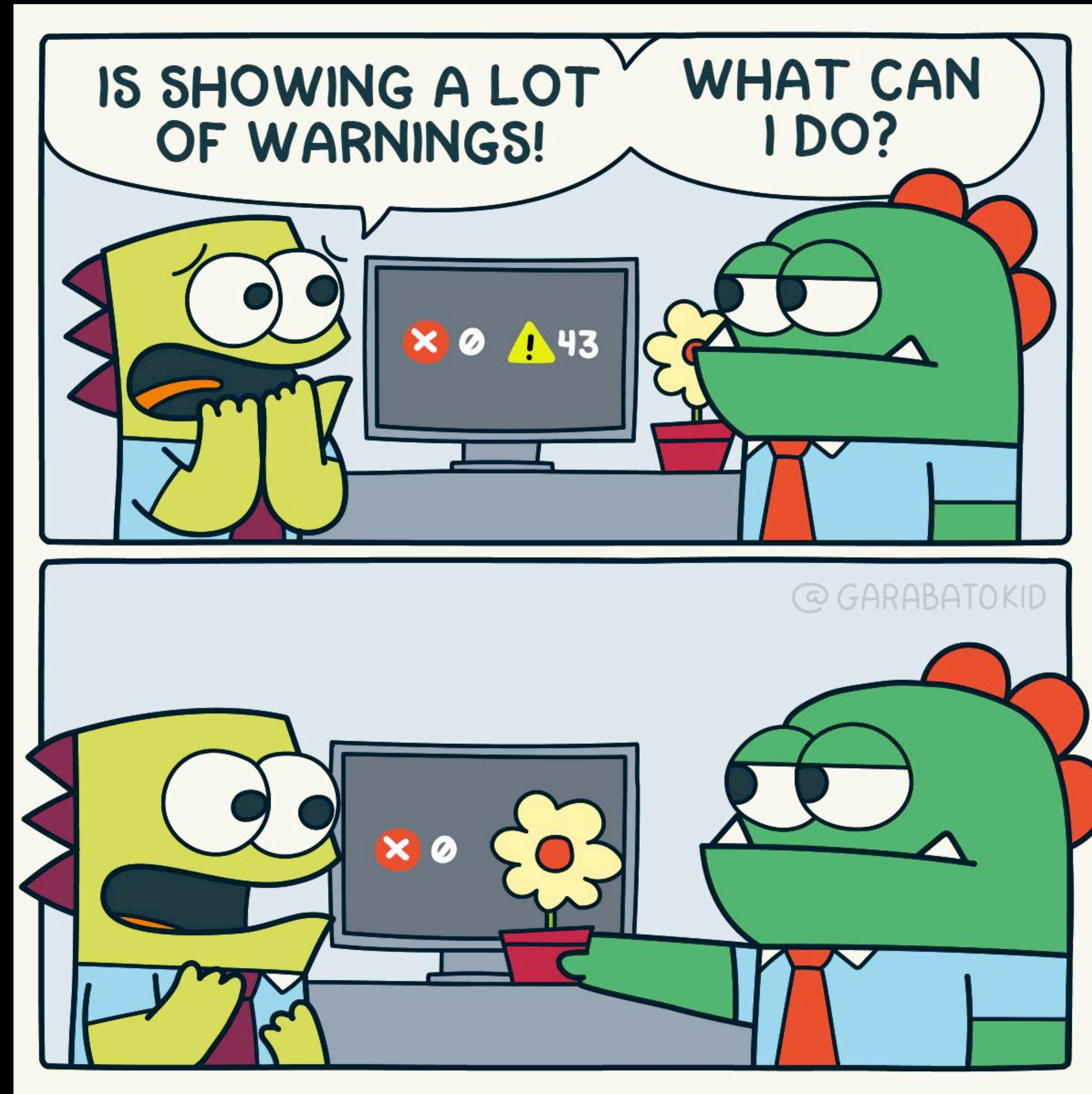
Anatomy of an attack

The alert chain



Signal to noise

Alert fatigue is the enemy



Signal to noise

What are we doing here?


Description

marcador package in PyPI 0.1 through 0.13 included a code-execution backdoor.

Severity

CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 **NIST: NVD** **Base Score: 9.8 CRITICAL** **Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

CVE Dictionary Entry:
[CVE-2022-28470](#)

NVD Published Date:
05/08/2022

NVD Last Modified:
05/17/2022

Source:
MITRE

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.


Hyperlink	Resource
http://pypi.doubanio.com/simple/request	Third Party Advisory
https://github.com/joajfreitas/marcador/issues/5	Exploit Issue Tracking Third Party Advisory
https://pypi.org/project/marcador/	Product

Signal to noise

What are we doing here?


Hyperlink	Resource
http://pypi.doubanio.com/simple/request	Third Party Advisory
https://github.com/joajfreitas/marcador/issues/5	Exploit Issue Tracking Third Party Advisory
https://pypi.org/project/marcador/	Product

Weakness Enumeration

CWE-ID	CWE Name	Source
NVD-CWE-noinfo	Insufficient Information	 NIST

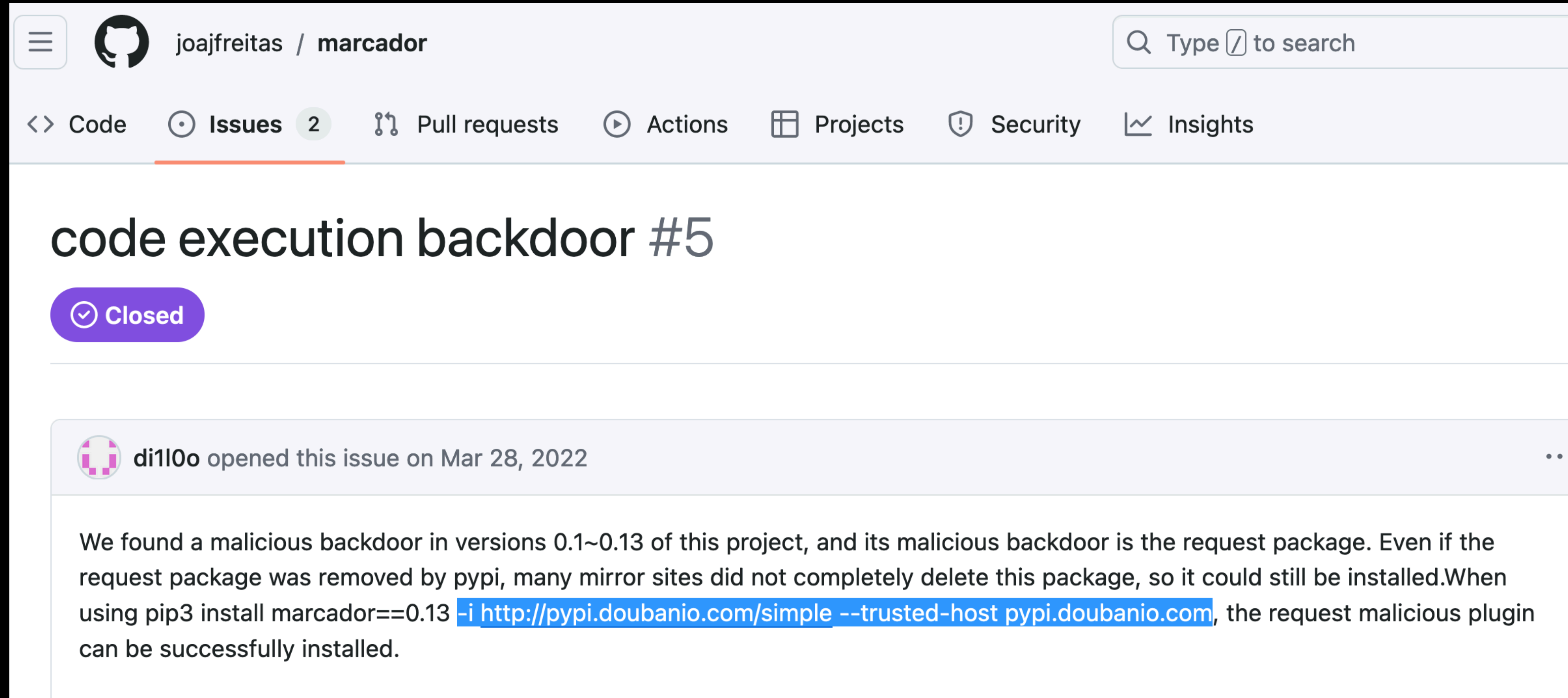
Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 ([hide](#))

 <code>cpe:2.3:a:python:pypi:*:*:*:*:*:*</code>	From (including)	Up to (including)
Show Matching CPE(s)	0.1	0.13

Signal to noise

What are we doing here?



joajfreitas / marcador

Code Issues 2 Pull requests Actions Projects Security Insights

code execution backdoor #5

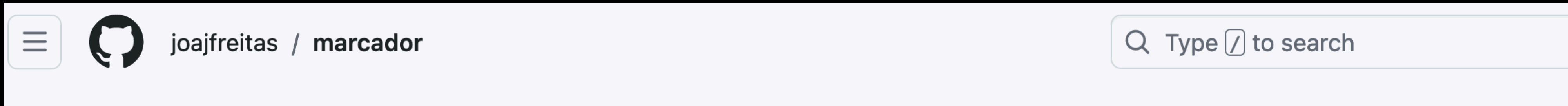
Closed

di1l0o opened this issue on Mar 28, 2022

We found a malicious backdoor in versions 0.1~0.13 of this project, and its malicious backdoor is the request package. Even if the request package was removed by pypi, many mirror sites did not completely delete this package, so it could still be installed. When using `pip3 install marcador==0.13 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com`, the request malicious plugin can be successfully installed.

Signal to noise

What are we doing here?



 joajfreitas on Mar 28, 2022

Owner ...

Just so I understand. You are using the <http://pypi.doubanio.com/simple> mirror when installing marcador. The malicious package is present in this mirror? Is it also present in the official pypi mirrors?

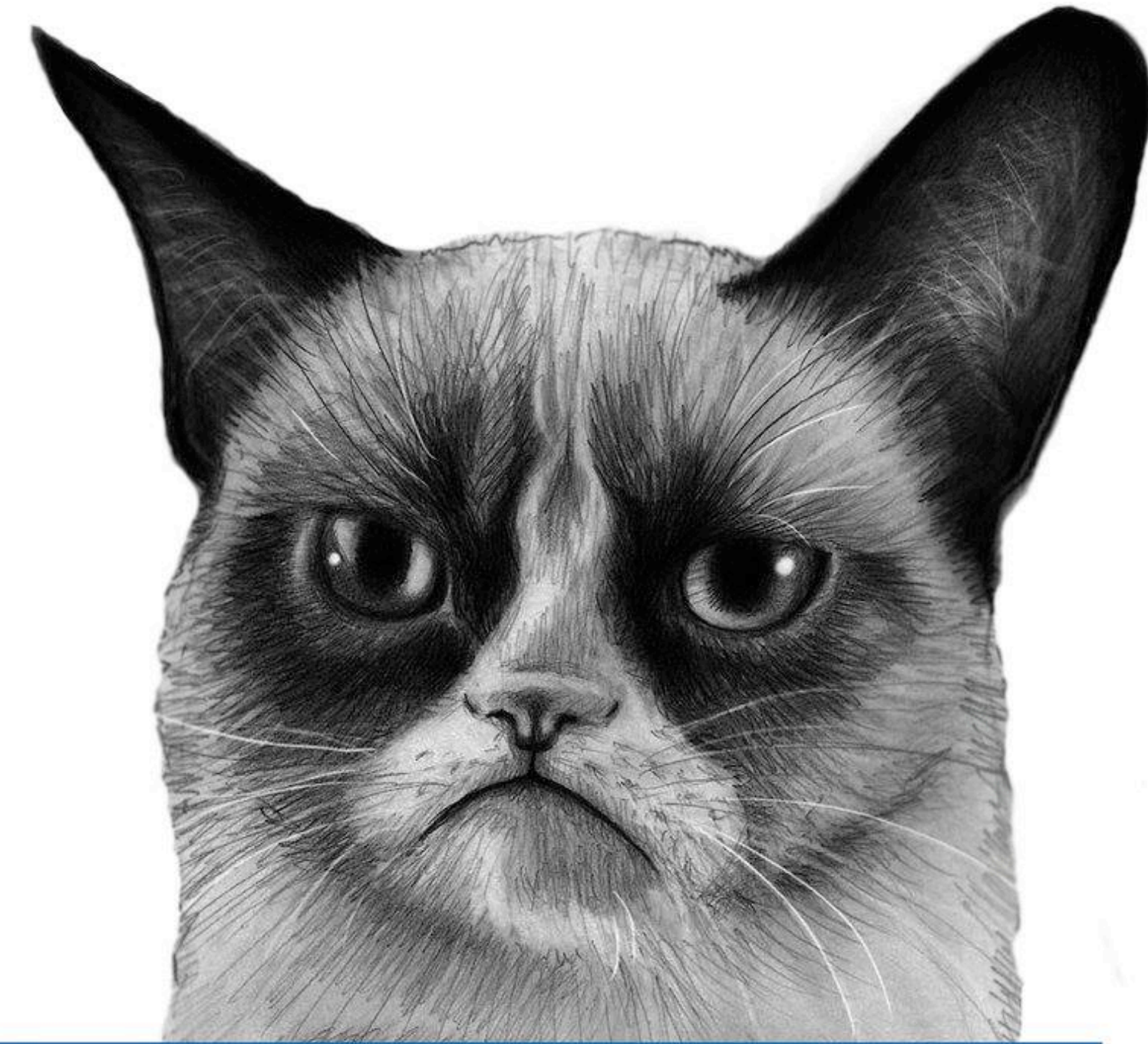
I see no problem in removing those versions from pypi just want to understand a bit better the thread model here :)



request package was removed by pypi, many mirror sites did not completely delete this package, so it could still be installed. When using `pip3 install marcador==0.13 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com`, the request malicious plugin can be successfully installed.

We cannot
expect better
unless we
enable better

You're a 10x hacker and it must be someone else's fault.



Blaming the User

Pocket Reference

ORLY?

@ThePracticalDev

How do we do that?

Where are we in the web?

- Our readers: Developers
 - We can inspect their source code
 - We cannot inspect their build systems
 - We cannot inspect their deploy environment

How do we do that?

What tools are at hand?

- We have source code to inspect
 - Manifest and lock files are common
 - We can know exactly what packages get used
 - We can know roughly what versions get used
 - We can model this in a database and index security claims

How do we do that?

The plan

- Index vulns on packages
 - Zero false positives by design
 - Quick delivery in the developer workflow
 - Common language to discuss vulns
 - Security claims are verifiable
 - Security claims are contestable

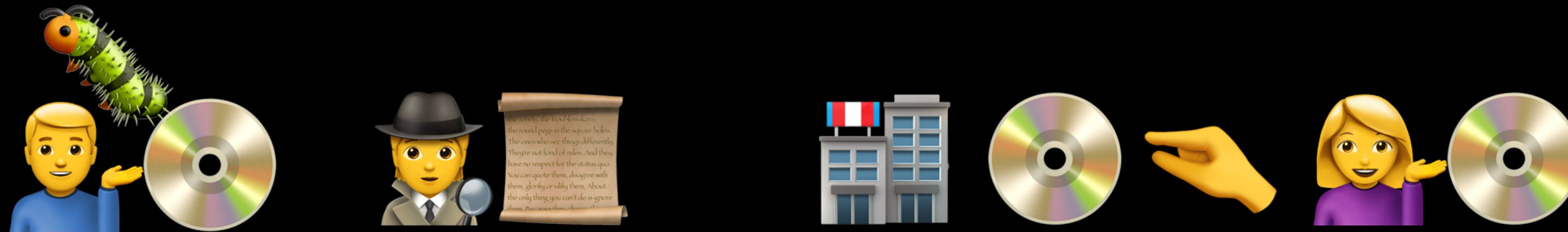
Anatomy of an advisory

The alert pipe



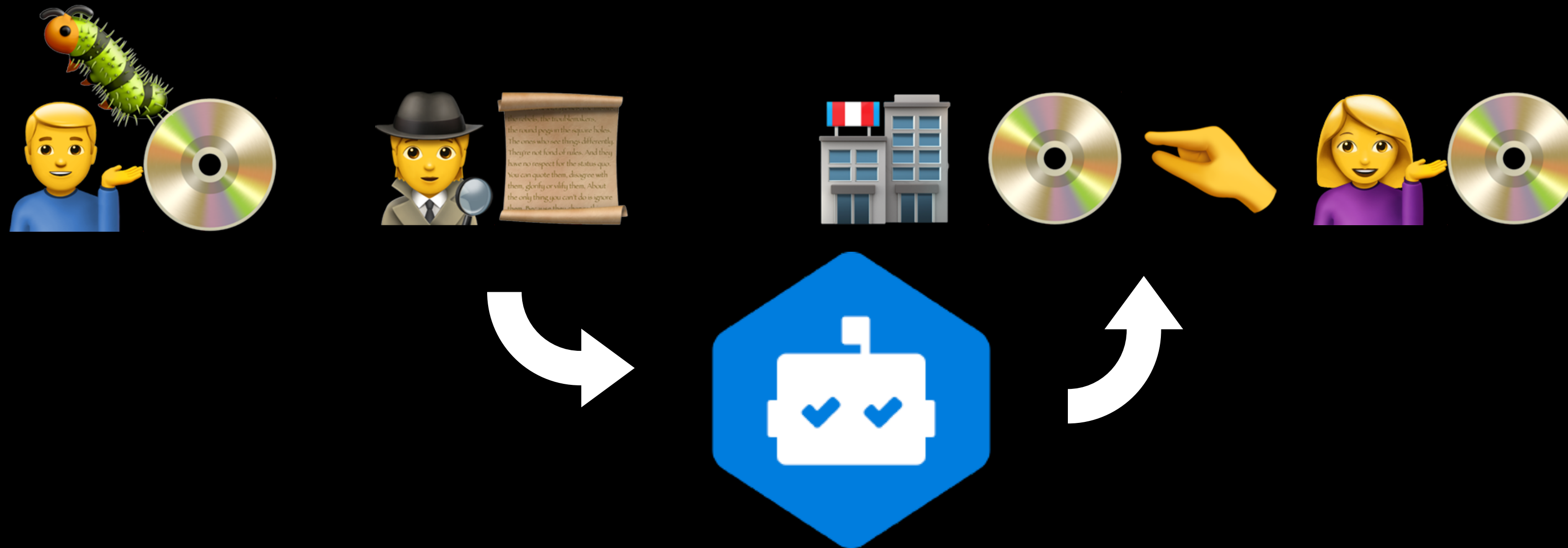
Anatomy of an advisory

The alert pipe



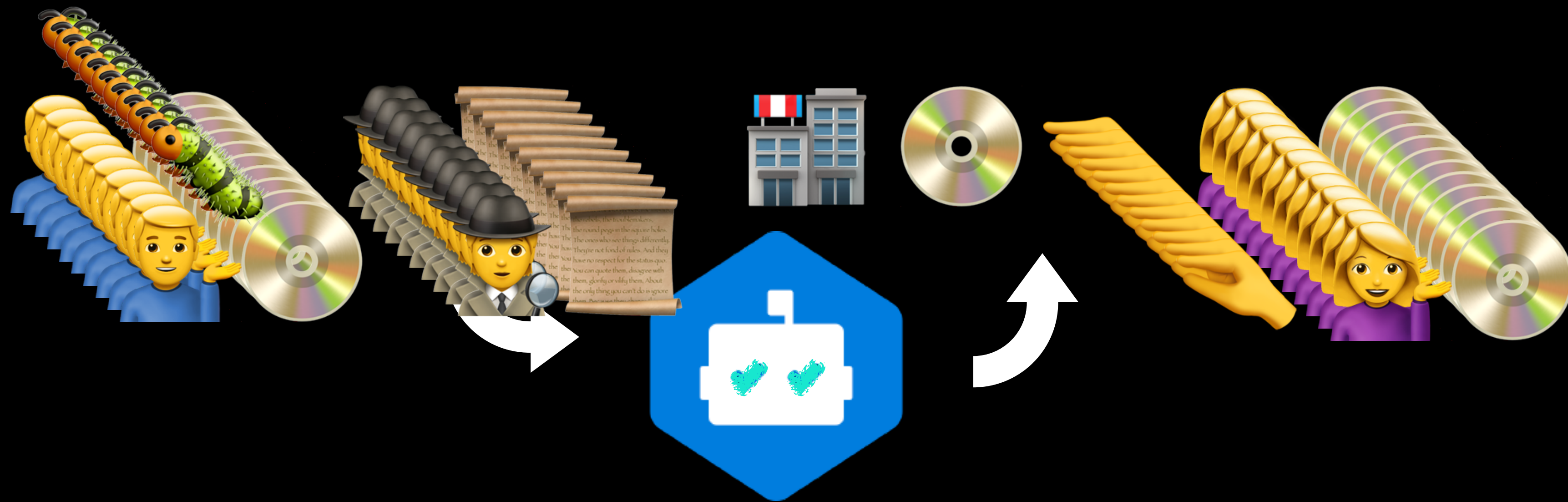
Anatomy of an advisory

The alert pipe



Anatomy of an advisory

And it scales

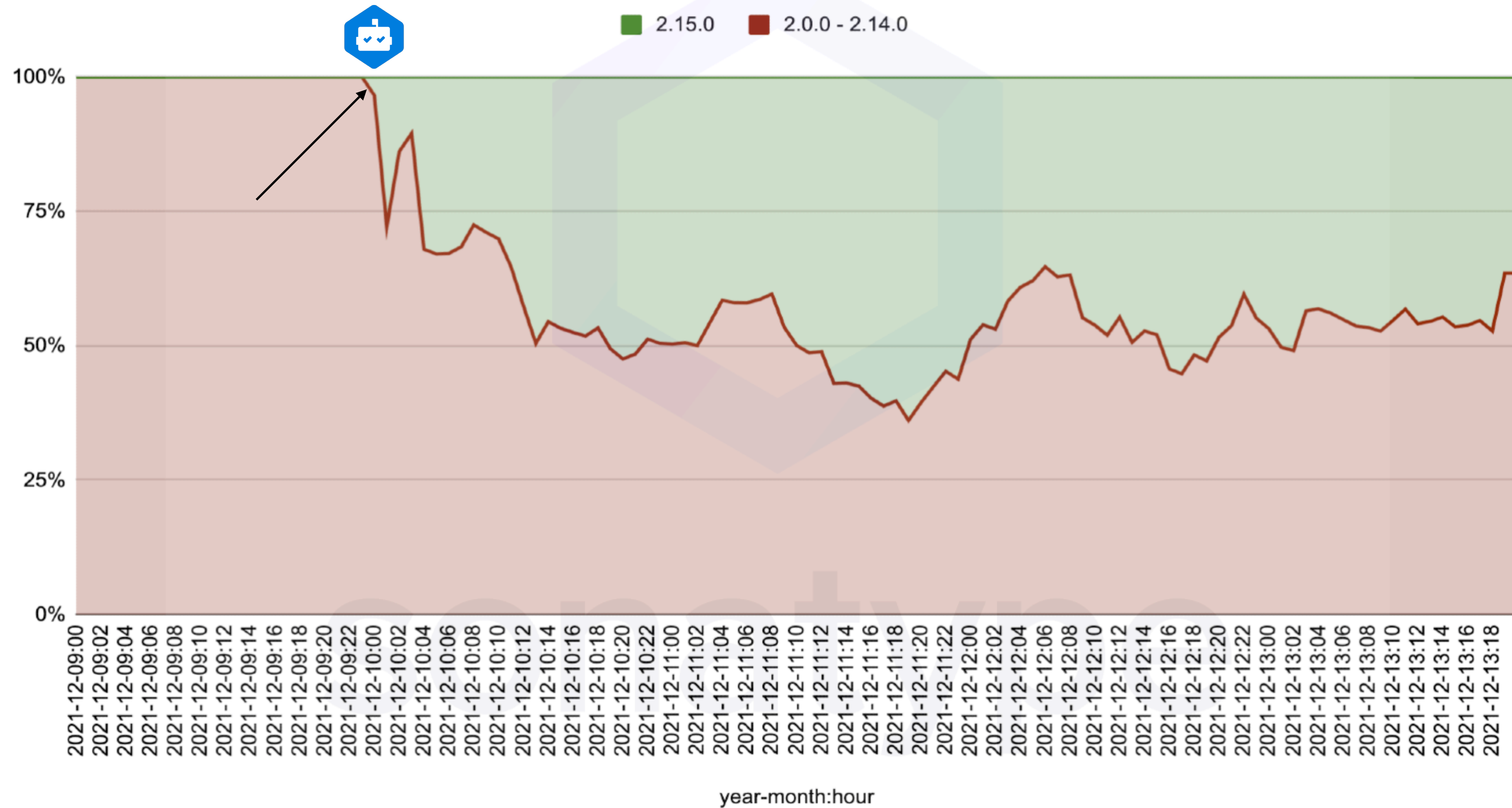


Alerts must flow

Fastest patch in the west!

other geos also supported!

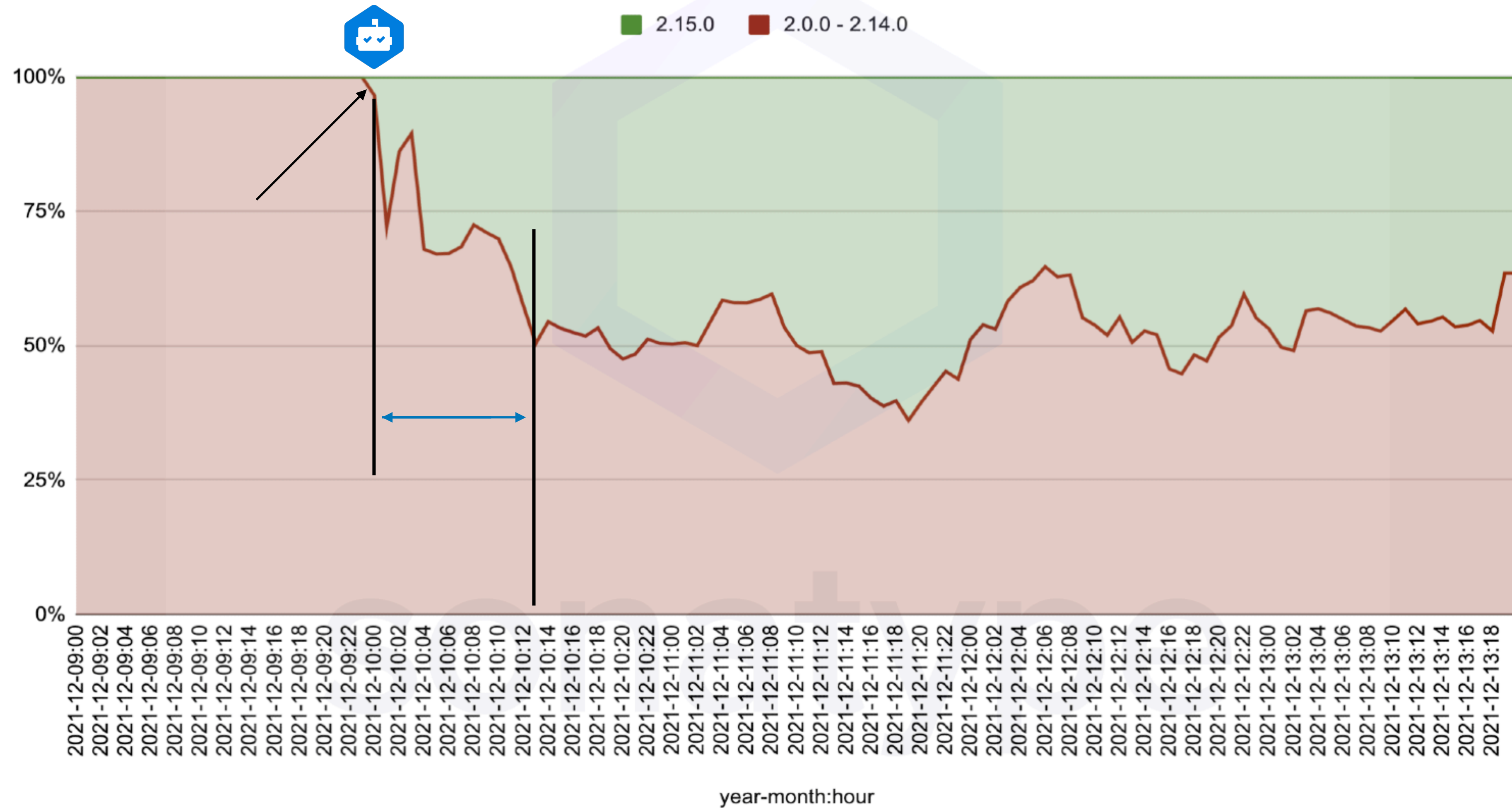
Log4J 2.x - hourly downloads after update released



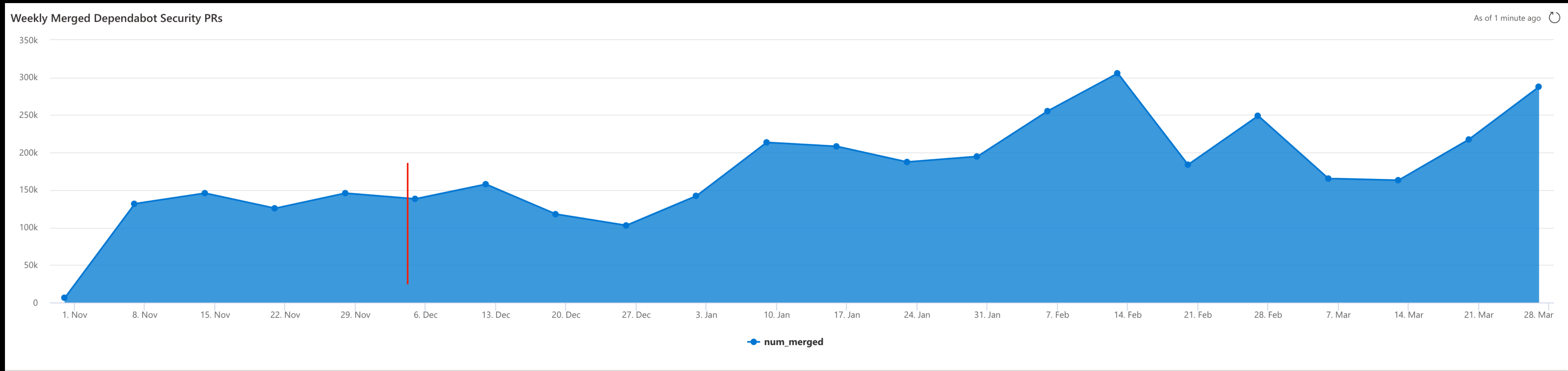
Fastest patch in the west!

other geos also supported!

Log4J 2.x - hourly downloads after update released



The long view



Open source


It's a trust building exercise



We are not perfect nor do we pretend to be

Does the advisory database cover other maven repositories? #2900

Open

 joshbressers opened this issue on Oct 31, 2023

As best as I can tell, most of the current Java packages cover Maven Central and not other maven repositories

For example the Atlassian maven repo

<https://packages.atlassian.com/content/repositories/atlassian-public/com/atlassian/>

contains confluence Java packages where Maven Central does not

<https://repo.maven.apache.org/maven2/com/atlassian/>


If we look at the MVN Repository site, we can see the top maven repositories

<https://mvnrepository.com/repos>

(there are shockingly more of these than I expected)

Thanks in advance



 darakian on Oct 31, 2023

Member

The short answer is `Sorta`. As of today our data should be considered to refer to objects on maven central only and if the package names and versions happen to be useful when read in the context of another registry then that's a happy accident. Longer term we've got a conversation going with OSV here [ossf/osv-schema#208](https://github.com/ossf/osv-schema/issues/208) on how to properly address the data which is happy accident today.



We get it wrong but we make it right

The screenshot shows a GitHub pull request titled "[GHSA-f8vr-r385-rh5r] hyper and h2 vulnerable to denial of service #2057". The pull request is merged and was created on April 12, 2023. It shows a commit history with a merge by 'advisory-database' and a commit by 'seanmonstar'. The main content is a comment from 'seanmonstar' discussing updates and comments regarding the vulnerability fix. The right sidebar shows metadata such as Reviewers, Assignees, Labels, Projects, Milestone, and Development status.

[GHSA-f8vr-r385-rh5r] hyper and h2 vulnerable to denial of service #2057 <> Code

Merged advisory-databa... merged 1 commit into seanmonstar/advisory-improvement-2057 from seanmonstar-GHSA-f8vr-r385-rh5r on Apr 12, 2023

Conversation 5 Commits 1 Checks 3 Files changed 1 +3 -22

seanmonstar commented on Apr 12, 2023

Updates

- Affected products
- Description
- Source code location

Comments

The code lives in the `h2` library, a fix will only require a new `h2` version. A `hyper` version will not need to be published, since hyper's dependency range allows the new version to be used once it exists.

Improve GHSA-f8vr-r385-rh5r 3b9270b

github-actions bot changed the base branch from `main` to `seanmonstar/advisory-improvement-2057` last year

advisory-database bot merged commit `cd971e5` into `seanmonstar/advisory-improvement-2057` on Apr 12, 2023
2 checks passed View details

Reviewers
No reviews

Assignees
No one—[assign yourself](#)

Labels
None yet

Projects
None yet

Milestone
No milestone


Development
Successfully merging this pull request may close these issues.
None yet

We can't do it all

The siren song of the tar pit

Unable to improve advisory database for C / C++ packages #2963

Open


 mswilson opened this issue on Nov 21, 2023

Indeed it is [documented in the README](#) that contributions are not accepted for advisories outside the supported ecosystems. But some of the most high-impact vulnerability bulletins that need improvements are in C and C++ packages that don't have an "ecosystem" as such. They are part of *all* the ecosystems.

I would really like to be able to improve [GHSA-mq29-j5xf-cjwr](#) in light of all the confusion seen in [madler/zlib#868 \(comment\)](#). But there's no way to do this.


What could possibly be done to improve these bulletins?

  7

 Neustradamus on Nov 21, 2023

An important ticket!



 darakian on Nov 22, 2023

Member edited by darakian · Edits · ...

They are part of all the ecosystems.

That's kinda the problem actually. Our ecosystems provide a one to one mapping between some package namespace and an advisory. We don't have false positives as a result and not having false positives (via dependency matching) results in more actionable advisories and better outcomes for developers receiving alerts.

What could possibly be done to improve these bulletins?

It's an open question and one that we're thinking about.

For what it's worth we do have plenty of advisories which are about C/C++ code which has been bundled into a package in one of our ecosystems

eg. <https://github.com/advisories?query=tensorflow+type%3Areviewed+ecosystem%3Apip>



We're on a journey
join us won't you?



Write advisories?

Call out your artifacts

The screenshot shows the Spring Security Advisories page for CVE-2024-22243. The page header includes the Spring logo and navigation links. The main heading is "CVE-2024-22243: Spring Framework URL Parsing with Host Validation". The severity is "HIGH" and the date is "FEBRUARY 21, 2024". The description states that applications using UriComponentsBuilder to parse external URLs may be vulnerable to open redirect or SSRF attacks. The affected products and versions are listed as Spring Framework 6.1.0-6.1.3, 6.0.0-6.0.16, and 5.3.0-5.3.31, along with older unsupported versions. Mitigation instructions advise upgrading to 6.1.4, 6.0.17, or 5.3.32. The credit section mentions Sean Pesce from Motorola Solutions.

Reporting
To report a security issue within the Spring ecosystem, please refer to the Spring Security Advisories page.

The screenshot shows the GitHub Advisory Database entry for CVE-2024-22243. The title is "Spring Web vulnerable to Open Redirect or Server Side Request Forgery". The severity is "High severity" and it is "GitHub Reviewed". The entry was published last week and updated 8 hours ago. The vulnerability details section shows the package "org.springframework:spring-web (Maven)" with affected versions ranging from 6.1.0 to 6.1.3 and patched versions 6.1.4, 6.0.17, and 5.3.32. The description repeats the information from the Spring Security Advisories page. The references section includes links to the NVD, Spring Security Advisories, and the GitHub source code.

GitHub Advisory Database / GitHub Reviewed / CVE-2024-22243

Spring Web vulnerable to Open Redirect or Server Side Request Forgery

High severity GitHub Reviewed Published last week to the GitHub Advisory Database • Updated 8 hours ago

Vulnerability details Dependabot alerts **29**

Package	Affected versions	Patched versions
org.springframework:spring-web (Maven)	$\geq 6.1.0, < 6.1.4$ $\geq 6.0.0, < 6.0.17$ $\geq 5.3.0, < 5.3.32$ $\leq 5.2.25.RELEASE$	6.1.4 6.0.17 5.3.32

Description

Applications that use UriComponentsBuilder to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to an open redirect attack or to a SSRF attack if the URL is used after passing validation checks.

References

- <https://nvd.nist.gov/vuln/detail/CVE-2024-22243>
- <https://spring.io/security/cve-2024-22243>
- <https://github.com/spring-projects/spring-framework/blob/main/spring-web/src/main/java/org/springframework/web/util/UriComponentsBuilder.java>

Read advisories?

Call out errors

Filters ▾ Labels 15 Milestones 0 [New pull request](#)

[Clear current search query, filters, and sorts](#)

0 Open ✓ 8 Closed	Author ▾	Label ▾	Projects ▾	Milestones ▾	Reviews ▾	Assignee ▾	Sort ▾
Update GHSA-r4q3-7g4q-x89m.json CVE-2024-22233 ✓							3
<small>#3365 by prabhu was closed on Feb 9</small>							
[GHSA-r4q3-7g4q-x89m] Spring Framework server Web DoS Vulnerability ✗							1
<small>#3338 by LukaszGrzesik was merged on Jan 24</small>							
[GHSA-r4q3-7g4q-x89m] Spring Framework server Web DoS Vulnerability ✗							1
<small>#3336 by tolmadis was merged on Jan 24</small>							
[GHSA-r4q3-7g4q-x89m] Spring Framework server Web DoS Vulnerability ✗							1
<small>#3335 by schmidt-fu was merged on Jan 24</small>							
[GHSA-r4q3-7g4q-x89m] Spring Framework server Web DoS Vulnerability ✗							1
<small>#3334 by fnxpt was merged on Jan 24</small>							
[GHSA-r4q3-7g4q-x89m] Spring Framework server Web DoS Vulnerability ✓							1
<small>#3332 by Yukilnu was closed on Jan 24</small>							
[GHSA-r4q3-7g4q-x89m] Spring Framework server Web DoS Vulnerability ✓							1
<small>#3331 by reva was closed on Jan 23</small>							
[GHSA-r4q3-7g4q-x89m] Spring Framework server Web DoS Vulnerability ✗							1
<small>#3330 by aruneko was merged on Jan 24</small>							

Want something we don't provide? Build it. If it's good they will come, we might help.



What do we do?

We're librarians 📚

We Can Do It!



GitHub Advisory Database

Security vulnerability database inclusive of CVEs and GitHub originated security advisories from the world of open source software.

GitHub reviewed advisories

All reviewed	14,490
Composer	2,242
Erlang	22
GitHub Actions	11
Go	1,214
Maven	3,951
npm	3,147
NuGet	510
pip	2,083
Pub	7
RubyGems	743
Rust	657
Swift	29

Unreviewed advisories

All unreviewed	197,394
----------------	---------

CC-BY-4.0 License

Language support ⓘ

About GitHub Advisory Database

Q Search by CVE/GHSA ID, package, severity, ecosystem, credit...

14,490 advisories

Severity ▾ CWE ▾ Sort ▾

Improper Control of Generation of Code ('Code Injection') in jai-ext Critical

CVE-2022-24816 was published for it.geosolutions.jaiext,jiffle:jt-jiffle (Maven) 1 hour ago

Pow Mnesia cache doesn't invalidate all expired keys on startup Moderate

CVE-2023-42446 was published for pow (Erlang) 4 hours ago

A remote command execution (RCE) vulnerability in the /api/runscript endpoint of FUXA High

CVE-2023-33831 was published for @frangoteam/fuxa (npm) yesterday

Vyper has incorrect re-entrancy lock when key is empty string Moderate

CVE-2023-42441 was published for vyper (pip) yesterday

Arbitrary File Overwrite in Eclipse JGit High

CVE-2023-4759 was published for org.eclipse.jgit:org.eclipse.jgit (Maven) yesterday

Cross-Site Request Forgery (CSRF) in usememos/memos High

CVE-2023-5036 was published for github.com/usememos/memos (Go) 2 days ago

Directus affected by VM2 sandbox escape vulnerability High

GHSA-22rr-f3p8-5gf8 was published for directus (npm) 4 days ago

Jetty's OpenId Revoked authentication allows one request Low

CVE-2023-41900 was published for org.eclipse.jetty:jetty-openid (Maven) 4 days ago

LibreNMS Cross-site Scripting vulnerability Critical

CVE-2023-4982 was published for librengms/librengms (Composer) 5 days ago

LibreNMS Cross-site Scripting vulnerability High

CVE-2023-4981 was published for librengms/librengms (Composer) 5 days ago

PRs welcome 👍
CC-BY-4.0 licensed!

We Can Do It!



<https://github.com/github/advisory-database#contributions>
<https://creativecommons.org/licenses/by/4.0/>

GitHub Advisory Database

Contributions

There are two ways to contribute to the information provided in this repository.

From any individual advisory on github.com/advisories, click **Suggest improvements for this vulnerability** (shown below) to open an "Improve security advisory" form. Edit the information in the form and click **Submit improvements** to open a pull request with your proposed changes.

See something to contribute? [Suggest improvements for this vulnerability](#)

Alternatively, you can submit a pull request directly against a file in this repository. To do so, follow the [contribution guidelines](#).

RubyGems	743	CVE-2023-4759 was published for org.eclipse.jgit:org.eclipse.jgit (Maven) yesterday
Rust	657	Cross-Site Request Forgery (CSRF) in usememos/memos High CVE-2023-5036 was published for github.com/usememos/memos (Go) 2 days ago
Swift	29	Directus affected by VM2 sandbox escape vulnerability High GHSA-22rr-f3p8-5gf8 was published for directus (npm) 4 days ago
Unreviewed advisories		
All unreviewed	197394	Jetty's OpenId Revoked authentication allows one request Low CVE-2023-41620 was published for org.eclipse.jetty:jetty-servlet (Java) 4 days ago
		LibreNMS Cross-site Scripting vulnerability Critical CVE-2023-41620 was published for libre/nms:libre-nms (Composer) 5 days ago
		LibreNMS Cross-site Scripting vulnerability High CVE-2023-4981 was published for librenms/librenms (Composer) 5 days ago

Help us improve our data, it's available for free, for everyone, forever.

- CC-BY-4.0 License
- Language support ⓘ
- About GitHub Advisory Database

Questions?

<https://github.com/github/advisory-database#contributions>

<https://creativecommons.org/licenses/by/4.0/>

We Can Do It!



GitHub Advisory Database

Contributions

There are two ways to contribute to the GitHub Advisory Database.

From any individual advisory on [github.com/advisories](#), click the **Improve this advisory** button (shown below) to open an "Improve security" form and click **Submit** improvements to open a pull request.

See something to contribute? [Suggest improvements for this vulnerability](#)

Alternatively, you can submit a pull request directly to this repository. To do so, follow the [contribution guidelines](#).



Help us improve our data, it's available for free, for everyone, forever.

RubyGems	743
Rust	657
Swift	29

Unreviewed advisories

All unreviewed 197,394

CC-BY-4.0 License

Language support

About GitHub Advisory Database

Cross-Site Request Forgery (CSRF) in `libreNMS` allows an attacker to impersonate an administrator and perform actions as an administrator. CVE-2023-5036 was published for libreNMS/libreNMS (Composer) 5 days ago

Directus authentication bypass in `directus` allows an attacker to bypass authentication and access all data. CVE-2023-4759 was published for directus/directus (Composer) yesterday

Jetty's OpenId Revoked authentication allows one request to be processed. CVE-2023-4981 was published for libreNMS/libreNMS (Composer) 5 days ago

LibreNMS Cross-site Scripting vulnerability (Critical) CVE-2023-4981 was published for libreNMS/libreNMS (Composer) 5 days ago

LibreNMS Cross-site Scripting vulnerability (High) CVE-2023-4981 was published for libreNMS/libreNMS (Composer) 5 days ago

Global API

Want to use our data for your own tools?

Global security advisories

Use the REST API to view global security advisories.

List global security advisories [↗](#)

✔ Works with [GitHub Apps](#)

Lists all global security advisories that match the specified parameters. If no other parameters are defined, the request will return only GitHub-reviewed advisories that are not malware.

By default, all responses will exclude advisories for malware, because malware are not standard vulnerabilities. To list advisories for malware, you must include the `type` parameter in your request, with the value `malware`. For more information about the different types of security advisories, see "[About the GitHub Advisory database.](#)"

Parameters for "List global security advisories"

Code samples for "List global security advisories"

GET /advisories

cURL JavaScript GitHub CLI

```
curl -L \  
-H "Accept: application/vnd.github+json" \  
-H "Authorization: Bearer <YOUR-TOKEN>" \  
-H "X-GitHub-API-Version: 2022-11-28" \  
https://api.github.com/advisories
```



Repo API

Want to get at raw user provided data?

Repository security advisories

Use the REST API to view and manage repository security advisories.

List repository security advisories for an organization [↗](#)

✔ Works with [GitHub Apps](#)

Lists repository security advisories for an organization.

To use this endpoint, you must be an owner or security manager for the organization, and you must use an access token with the `repo` scope or `repository_advisories:write` permission.

Parameters for "List repository security advisories for an organization"

Headers

accept string
Setting to `application/vnd.github+json` is recommended.

Path parameters

org string **Required**
The organization name. The name is not case sensitive.

Query parameters

Code samples for "List repository security advisories for an organization"

GET `/orgs/{org}/security-advisories`

cURL JavaScript GitHub CLI

```
curl -L \
-H "Accept: application/vnd.github+json" \
-H "Authorization: Bearer <YOUR-TOKEN>" \
-H "X-GitHub-API-Version: 2022-11-28" \
https://api.github.com/orgs/ORG/security-advisories
```

Response

Example response Response schema

Status: 200

```
[
  {
    "ghsa_id": "GHSa-abcd-1234-efgh",
    "cve_id": "CVE-2050-00000",
    "url": "https://api.github.com/repos/repo/a-package/security-advisories/GHSa-abcd-1234-efgh"
```



Private Vulnerability Reporting

Want to not have 0 days dropped on you?

Configuring private vulnerability reporting for a repository

Owners and administrators of public repositories can allow security researchers to report vulnerabilities securely in the repository by enabling private vulnerability reporting.

Who can use this feature

Anyone with admin permissions to a public repository can enable and disable private vulnerability reporting for the repository.

About privately reporting a security vulnerability [↗](#)

Security researchers often feel responsible for alerting users to a vulnerability that could be exploited. If there are no clear instructions about contacting maintainers of the repository containing the vulnerability, security researchers may have no other choice but to post about the vulnerability on social media, send direct messages to the maintainer, or even create public issues. This situation can potentially lead to a public disclosure of the vulnerability details.



Dismissal Rules

Want to fine tune what alerts you see?

Using alert rules to prioritize Dependabot alerts

You can use Dependabot alert rules to filter out false positive alerts or alerts you're not interested in.

Who can use this feature

People with write permissions can view Dependabot alert rules for the repository. People with with admin permissions to a repository, or the security manager role for the repository, can enable or disable Dependabot alert rules for the repository, as well as create custom alert rules.

Note: Dependabot alert rules are currently in beta and are subject to change.

