

# Let's work for free

It's fun, sometimes.

**Christian Grobmeier**  
**Mastodon: mastodon.social/@grobmeier**  
**<https://grobmeier.solutions>**



# Who are you again?

*Christian Grobmeier*

1 Wife, 1 Kid, 1 Horse

Self employed

Authoring a book on Java Logging for Manning

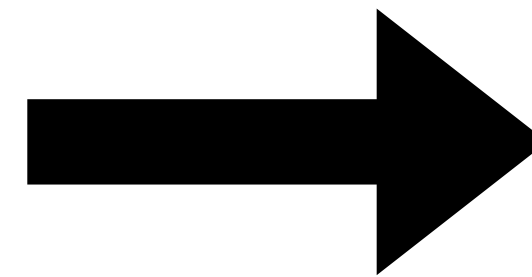
Apache Software Foundation Member

Current VP Data Privacy

Ex-VP Logging Services

Committer to log4php, log4j 1, log4j2


Contributions to many other Open Source projects



Mastodon: [mastodon.social/@grobmeier](https://mastodon.social/@grobmeier)

# Why are you doing open source?

Here is a pro and contra list!

- No money :-)
  - Lot's to learn
  - Making new friends
  - Finding good jobs
  - Trying out new things
- 
- No money :-)
  - Too much to learn
  - Meeting people you don't like
  - Getting ridiculous job offers
  - Trying to make everybody happy



**Open Source should be fun.**

ALL MODERN DIGITAL  
INFRASTRUCTURE

All thankless?

React

Spring

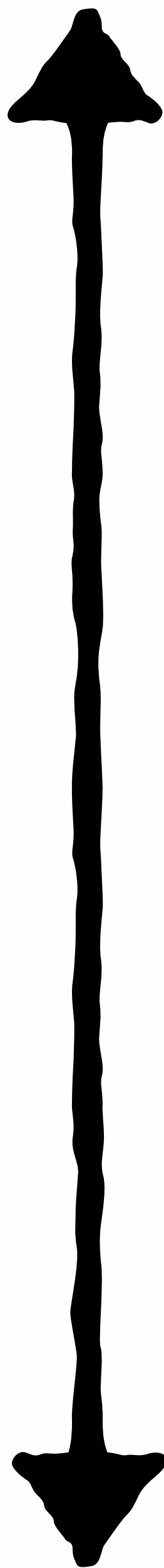
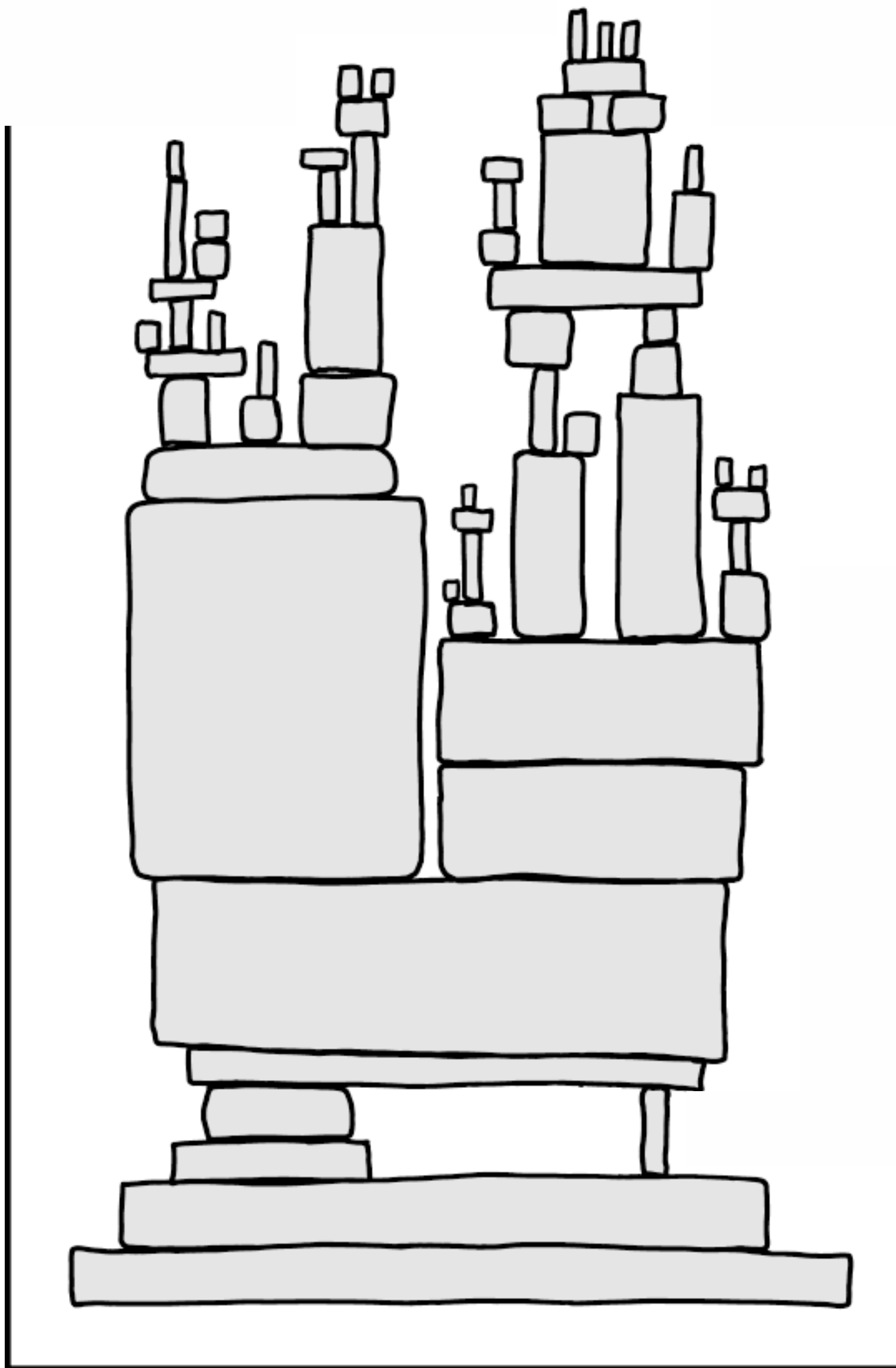
PostgresQL

A PROJECT SOME  
RANDOM PERSON  
IN NEBRASKA HAS  
BEEN THANKLESSLY  
MAINTAINING  
SINCE 2003

Hadoop

Log4j

Kubernetes



### Cool and fancy stuff

Crypto Wallets  
Online Spreadsheets

NFT  
Pokemon Mobile

Online Banking  
Solar Panel Monitoring

### Impressive tech

Angular  
Hadoop

React

MongoDB  
Kafka

Typescript

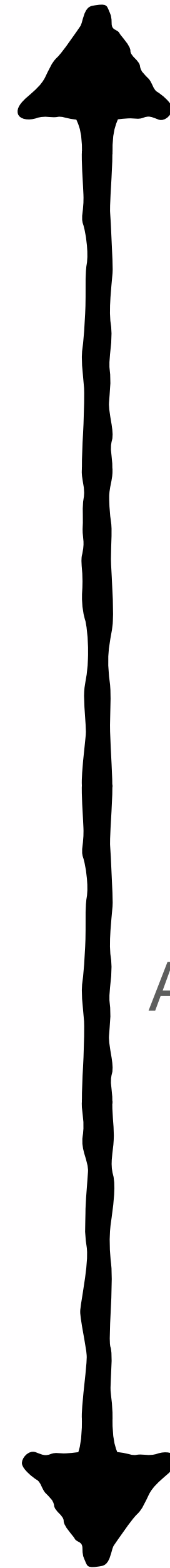
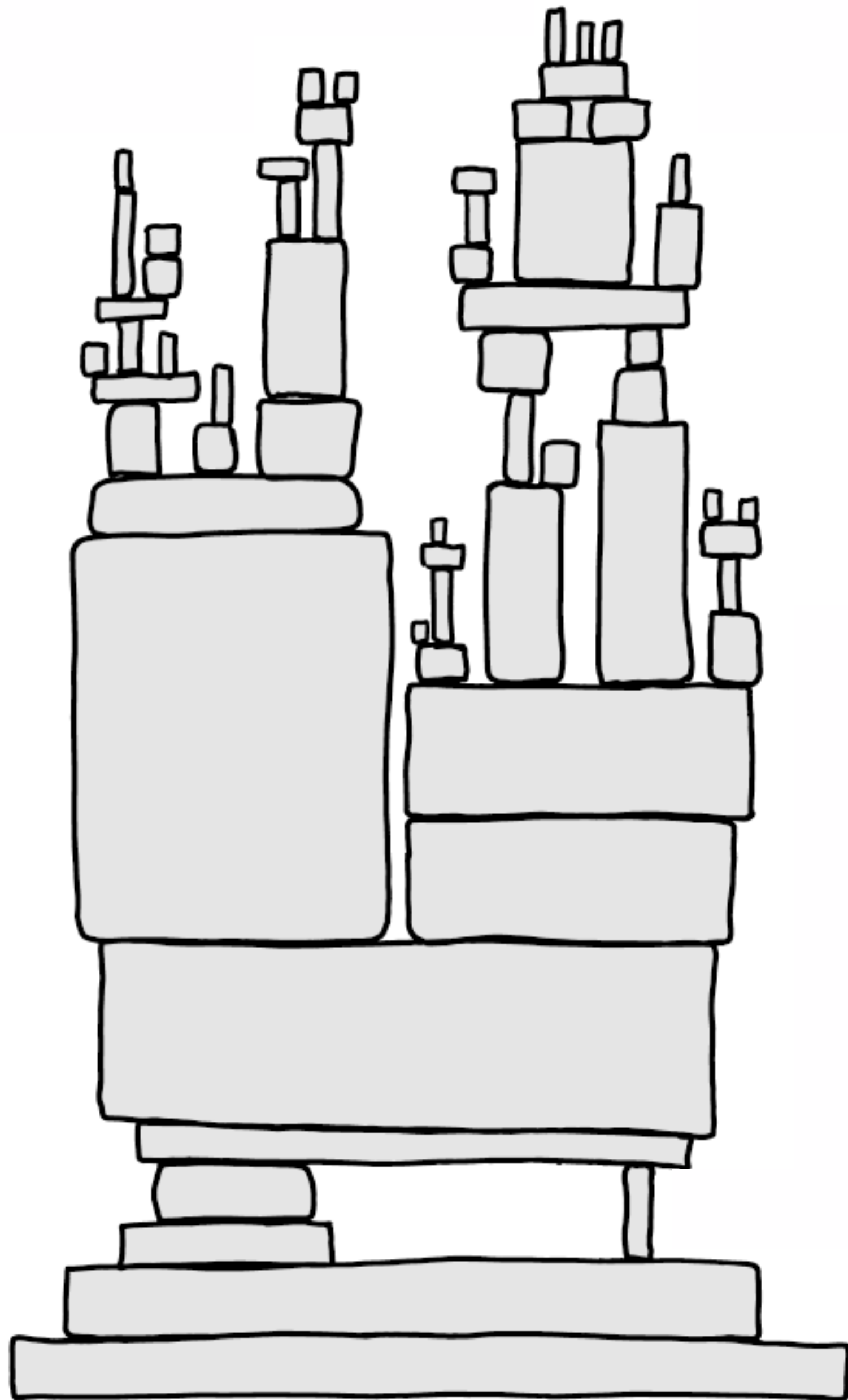
### Boring stuff

Log4j

### Expert World

JDK  
Dart Lang

Things nobody can spell out  
Ethereum VM



Funding for ~13 years of service:

0 \$

Log4j Team:

Pre-Incident: a few bucks

After Incident: some donations via GitHub or directly

One year after incident: Some GitHub sponsoring



What about...



Apache SpamAssassin™





**Log4(s)hell**

**Let's talk about it.**

# Understanding Log4j versions:

2001 - 2015 Log4j **1**  
(**unaffected** by log4shell)

2014 - now Log4j **2**  
(rewrite of Log4j 1, **affected**)

~6 active maintainers

Until 2021 far, Log4j was a low profile project

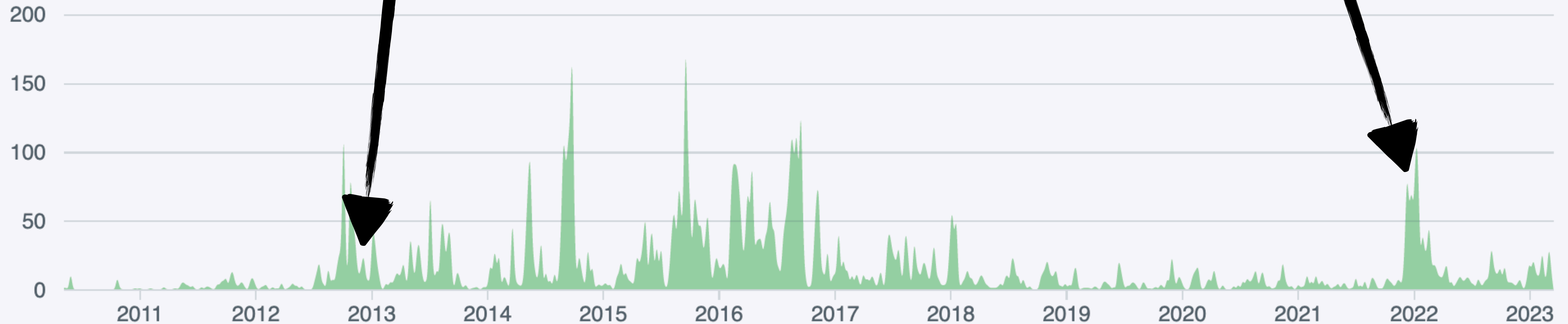
# Why did we have this incident?

The feature was created in July 2013,  
before the first release of Log4j 2.  
It was feature 313 from an outside contributor.

Years later, JNDI-related issues were  
discussed at a security conference.  
The information never reached us.

log4shell was born

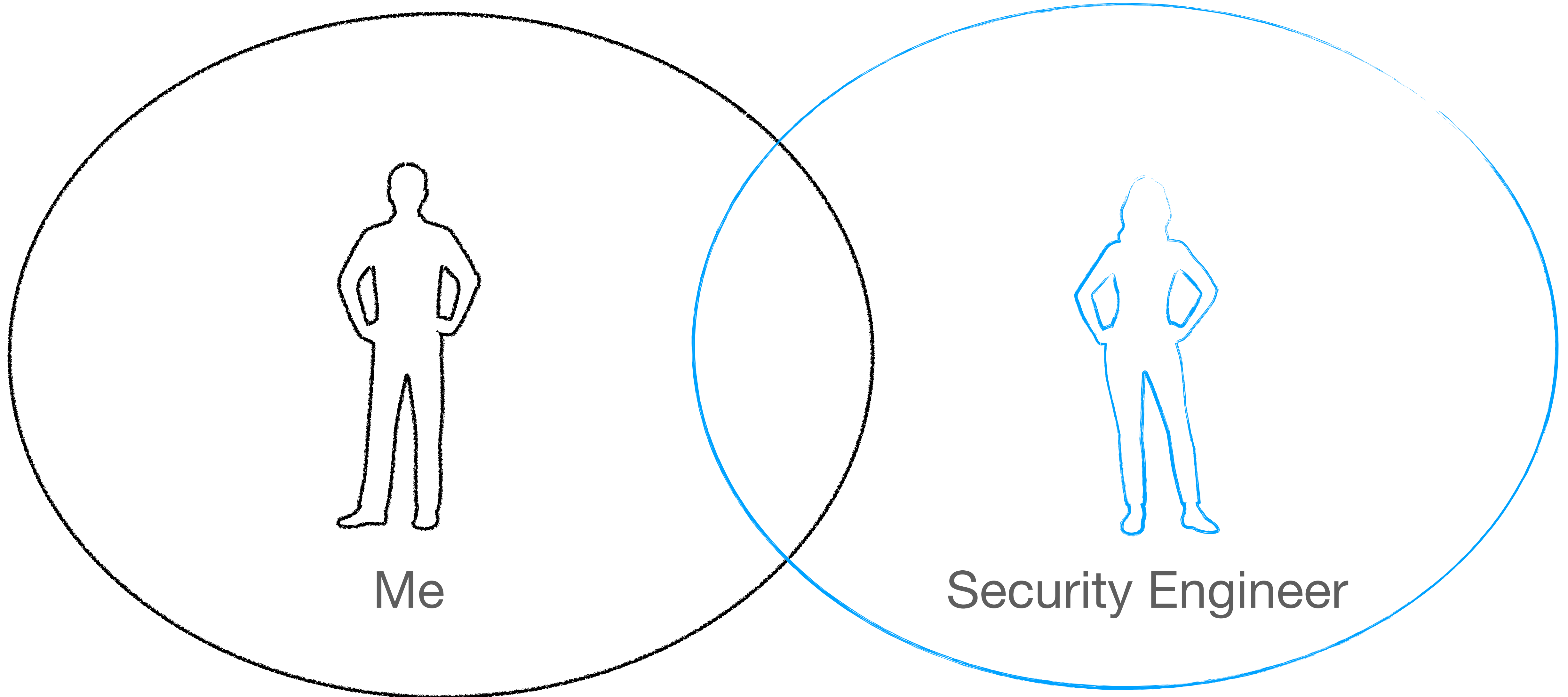
log4shell was found



Project activity on GitHub

Blackhat Conf on JNDI Injection

# Why did you not see this?



Me

Security Engineer

# Timeline of log4shell

2021-11-24 - First report of issue

2021-11-25 - Issue acknowledged

Known affected projects: Apache Flink, Apache Druid, Apache Struts 2

2021-11-29 - Issue understood and solution discussed

2021-12-05 - Issue solved - Release vote started

2021-12-08 - **(Public) security groups started to talk about it on social media**

2021-12-09 - Reporter was able to bypass the fix, vote cancelled

# Timeline of log4shell

2021-12-09 - New release candidate prepared

More vulnerability reports for RC1 were sent

2021-12-10 - Log4j 2.15.0 was released (fast track)

2021-12-11+ - More reports came in several more releases created

Things we experienced



# Was it a good idea to not pay our devs?

What people



Things which happened in the first days:

Tons of private messages

Meetings on Slack

Releasing multiple versions

Dealing with many other security reports

Some of us worked almost 24h in a row.

# Some “constructive” feedback

**Das Problem ist schlicht und ergreifend, dass der gemeine Java Entwickler nix ka**

Der Grund für die Entwicklung von Java war eine Öffnung der Softwareentwicklung für viele unerfahrene, insbesondere billigste Entwickler weltweit.

Die sog. 'Coder'

Beliebig ersetzbare Menschen, die eigentlich nichts können müssen.

Das ist DIE Ursache des hypes Java.

Ein Versuch der IT sich zu industrialisieren.

Jetzt stockt der Atem.

Diese billigen, dummen Leute produzieren jetzt ihren eigenen Wildwuchs.

Code, der aus der lokalen Perspektive wünschenswert erscheint, aber eigentlich unverantwortlich ist.

Es ist schlicht-und-ergreifend die verdiente späte Rache für die Accentures und EYs dieser Welt.

Auch dafür sollte man Sie zur Rechenschaft ziehen ..

**Re: Panikmache**

Absolut. Das klingt wirklich wie Panikmache. Von einer imaginären Gefahr reden die in der Zukunft liegt die wir jetzt unbedingt abwenden müssen. Böse Zungen munkeln das erinnert uns an Corona.

The Log4j Team  
DESTROYED MY WEEKEND!!!

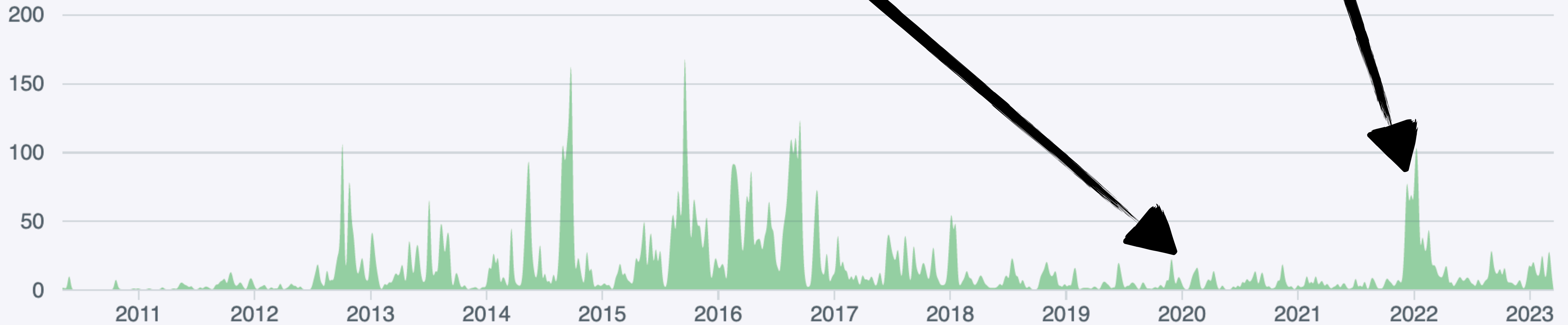
```
INFO] | +- jakarta.persistence:jakarta-persistence-api:jar:2.2.3:compile
INFO] | +- org.hibernate:hibernate-core:jar:5.6.4.Final:compile
INFO] | | +- org.jboss.logging:jboss-logging:jar:3.4.3.Final:compile
INFO] | | +- net.bytebuddy:byte-buddy:jar:1.11.22:compile
INFO] | | +- antlr:antlr:jar:2.7.7:compile
INFO] | | +- org.jboss:jandex:jar:2.4.2.Final:compile
INFO] | | +- com.fasterxml:classmate:jar:1.5.1:compile
INFO] | | +- org.hibernate.common:hibernate-commons-annotations:jar:5.1.2.Final:compile
INFO] | | \- org.glassfish.jaxb:jaxb-runtime:jar:2.3.5:compile
INFO] | |   +- org.glassfish.jaxb:txw2:jar:2.3.5:compile
INFO] | |   +- com.sun.istack:istack-commons-runtime:jar:3.0.12:compile
INFO] | |   \- com.sun.activation:jakarta.activation:jar:1.2.2:runtime
INFO] | +- org.springframework.data:spring-data-jpa:jar:2.6.1:compile
INFO] | | +- org.springframework.data:spring-data-commons:jar:2.6.1:compile
INFO] | | +- org.springframework:spring-orm:jar:5.3.15:compile
INFO] | | +- org.springframework:spring-context:jar:5.3.15:compile
INFO] | | +- org.springframework:spring-tx:jar:5.3.15:compile
INFO] | | +- org.springframework:spring-beans:jar:5.3.15:compile
INFO] | | \- org.slf4j:slf4j-api:jar:1.7.33:compile
INFO] | \- org.springframework:spring-aspects:jar:5.3.15:compile
INFO] +- org.springframework.boot:spring-boot-starter-web:jar:2.6.3:compile
INFO] | +- org.springframework.boot:spring-boot-starter:jar:2.6.3:compile
INFO] | | +- jakarta.annotation:jakarta.annotation-api:jar:1.3.5:compile
INFO] | | \- org.yaml:snakeyaml:jar:1.29:compile
INFO] | +- org.springframework.boot:spring-boot-starter-json:jar:2.6.3:compile
INFO] | | +- com.fasterxml.jackson.core:jackson-databind:jar:2.13.1:compile
INFO] | | | +- com.fasterxml.jackson.core:jackson-annotations:jar:2.13.1:compile
INFO] | | | \- com.fasterxml.jackson.core:jackson-core:jar:2.13.1:compile
INFO] | | +- com.fasterxml.jackson.datatype:jackson-datatype-jdk8:jar:2.13.1:compile
INFO] | | +- com.fasterxml.jackson.datatype:jackson-datatype-jsr310:jar:2.13.1:compile
INFO] | | \- com.fasterxml.jackson.module:jackson-module-parameter-names:jar:2.13.1:compile
INFO] | +- org.springframework.boot:spring-boot-starter-tomcat:jar:2.6.3:compile
INFO] | | +- org.apache.tomcat.embed:tomcat-embed-core:jar:9.0.56:compile
INFO] | | +- org.apache.tomcat.embed:tomcat-embed-el:jar:9.0.56:compile
INFO] | | \- org.apache.tomcat.embed:tomcat-embed-websocket:jar:9.0.56:compile
```

People don't  
**know**  
if they have a  
**problem.**

Do you see the  
issues in your  
Spring Boot App  
with 115 deps?

When we started to think Log4j was on Mars

When Nasa told us Log4j is not on Mars



Project activity on GitHub

# Log4j Vulnerable Downloads Dashboard

Screenshot  
from 20.03.2023.

34% of daily  
downloads use  
vulnerable versions

log4j Latest Statistics

# 158,811,270

Total Downloads Since Dec 10, 2021

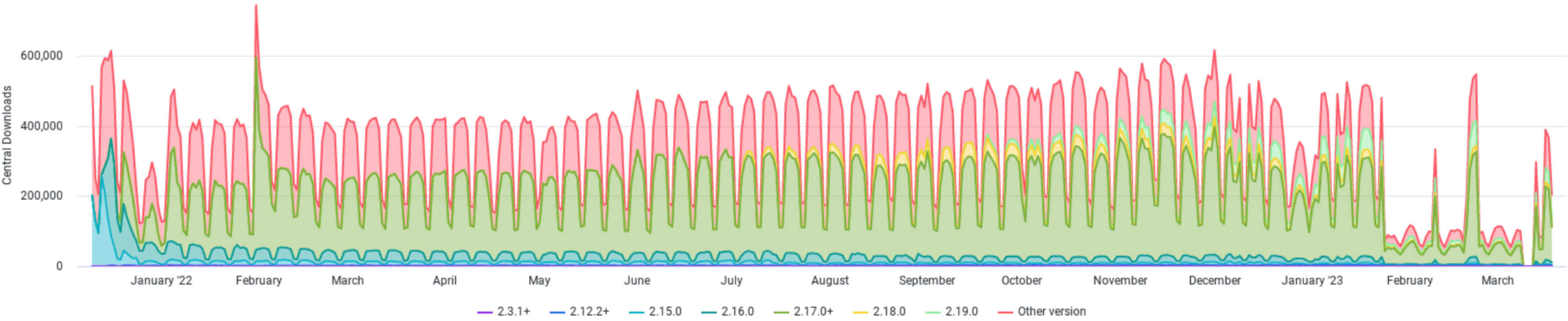
33 % vulnerable

# 34 %

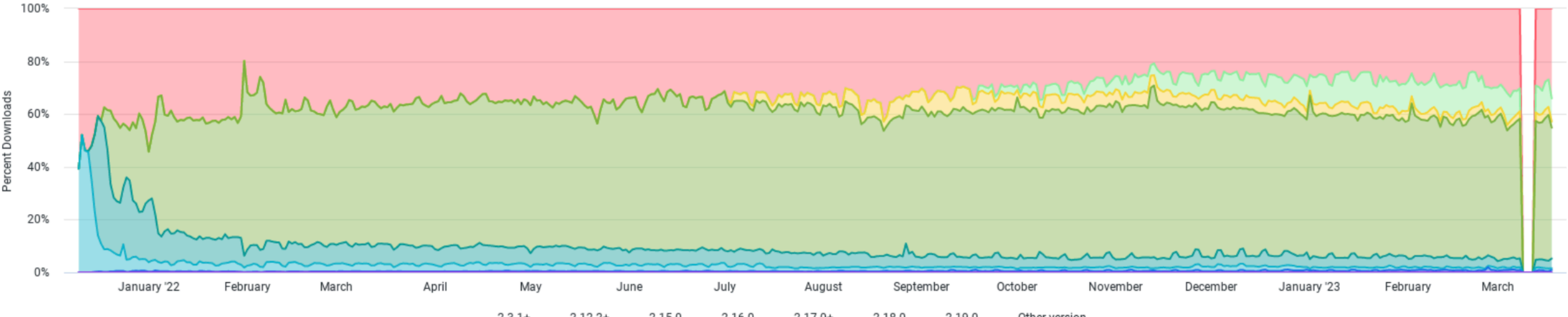
Vulnerable Downloads Last 24 Hours

203,707 total downloads

log4j Daily Central Downloads



log4j Percent Daily Central Downloads



FAQ around 2021:

Should I use Log4j 1?

Why did you not restart Log4j 1?

Can you fix 10 year old “security issues” too?

I am playing Minecraft, is this a problem?

Press: what is going to explode?

## Lessons learned:

When you report security issues,  
your government may harm you.

Chinese gov punished Alibaba.  
CDU sued the reporter of the CDU Connect problem.



## Lessons learned:

Log4j 3 will have “opt-in” features and provide modules.

People don't update.

## Today:

Log4j2 is “safe”: many people helped to find issues

Improved migration paths from old versions

A new committer joined after the issue

[security@logging.apache.org](mailto:security@logging.apache.org) was created

Security is still coordinated by the ASF security team

**Thank you for your service**



# Log4j

Enhancing security, stability,  
and confidence in Java logging

## Key facts

Status:

CURRENT

Investment Amount

€596,160.00

Investment Year(s)

2023, 2024

[logging.apache.org](https://logging.apache.org) →

[Repository](#) →

# Different money different problems

Speed

Paid versus unpaid

People are people

Taxes

# Thanks!

Mastodon: [mastodon.social/@grobmeier](https://mastodon.social/@grobmeier)

LinkedIn: <https://www.linkedin.com/in/grobmeier/>

Web: <https://grobmeier.solutions>

Email: [cg@grobmeier.de](mailto:cg@grobmeier.de)

# Image Credits

- Money: JP Valery (<https://unsplash.com/photos/time-lapse-photography-of-several-burning-us-dollar-banknotes-blOLCO2K4M0>)
- Koala: Lennart Nacke (<https://unsplash.com/photos/gray-koala-on-branch-G4Mgm1Tnfw4>)
- Eric Mclean (<https://unsplash.com/photos/a-person-holding-a-cookie-with-a-face-painted-on-it-qYV86rlxHLQ>)
- Climber: Jeff Ochoa [https://unsplash.com/photos/53S-oN\\_r9SU](https://unsplash.com/photos/53S-oN_r9SU)
- Speak Truth: Brett Jordan <https://unsplash.com/photos/Pd3ml1YRPIg>
- Kids talking: [saeed karimi https://unsplash.com/photos/JrrWC7Qcmhs](https://unsplash.com/photos/JrrWC7Qcmhs)
- Beach Yoga: [Chelsea Gates https://unsplash.com/photos/n8L1VYaypcw](https://unsplash.com/photos/n8L1VYaypcw)
- Chicken: [chatnarin pramnapan https://unsplash.com/photos/hsnelnK7mt4](https://unsplash.com/photos/hsnelnK7mt4)

License of this presentation: CC-BY-SA 4.0

Images used from Unsplash may have a different license.