



Who are these Open Source maintainers, actually?

A Drama with Happy End

Marak Squires

npm libraries 'colors' and 'faker' sabotaged in protest by their maintainer—What to do now?

January 10, 2022 By Ax Sharma
7 minute read time

r/cscareerquestions • vor 2 Jahren
HexadecimalCowboy

LOG4J HAS OFFICIALLY RUINED MY WEEKEND

Experienced

LOG4J HAS OFFICIALLY RUINED MY FUCKING WEEKEND. THEY HAD TO REVEAL THIS EXPLOIT ON THE FRIDAY NIGHT THAT I WAS ON-CALL. THEY COULD NOT WAIT 2 FUCKING DAYS BEFORE THEY GREW A THICK GIRTHY CONSCIENCE AND FUCKED ME WITH IT? ALSO WHAT IS THEIR FUCKING DAMAGE WITH THIS LOGGING PACKAGE BEING A DAY-0 EXPLOIT? WHY IS A LOGGING PACKAGE DOING ANYTHING BESIDES. SIMPLY. LOGGING. THE. FUCKING. STRING? YOU DICKS HAD **ONE** JOB. NO THEY HAD TO MAKE IT SO IT COULD EXECUTE ARBITRARILY FORMATTED STRINGS OF CODE OF COURSE!!!!!! FUCK LOGGING. FUCK JAVA. AND FUCK THAT MINECRAFT SERVER WHERE THIS WAS DISCOVERED.

CVE-2024-3094 is a vulnerability discovered in the open-source library XZ Utils that stems from malicious code that was pushed into the library by one of its maintainers.

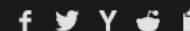
Mainly Ralph Goers and Christian Grobmeier

Lasse Collin

EXPLOIT THE STRESSED-OUT PACKAGE MAINTAINER, EXPLOIT THE SOFTWARE PACKAGE

by: Donald Papp

10 Comments



March 31, 2024



Call Incoming...



Meet Alex, a young developer. Alex is new to the Open Source world, but they got a lot of passion and a clear vision: to create a tool that helps people develop software more productively. Alex starts as a one-person team, driven by their own needs and desire to create something better, and starts writing code.

What drives Alex?



Intrinsic Motivation

- Autonomy
- Mastery
- Purpose

„Scratching your own itch“

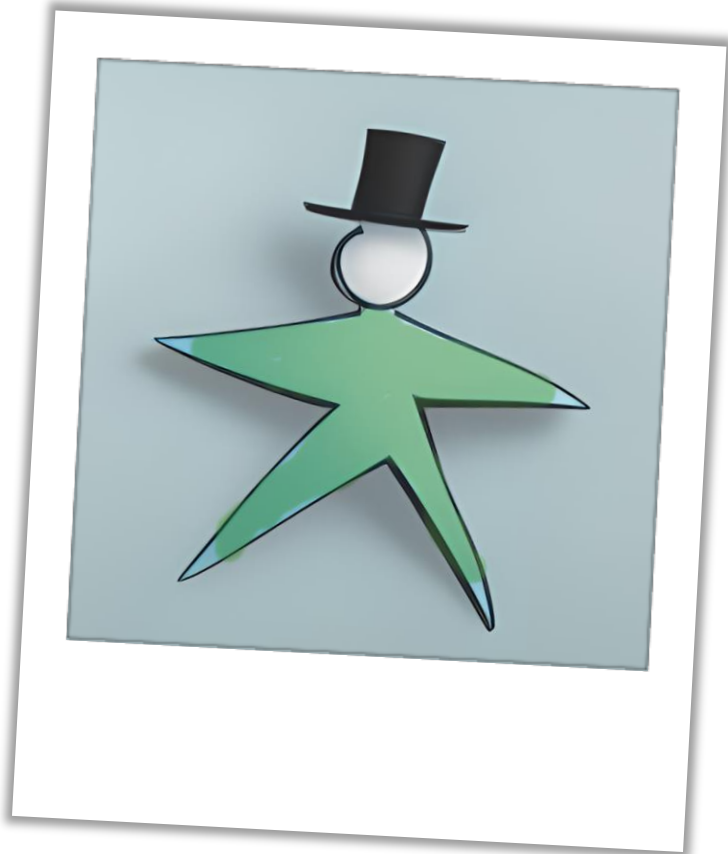
- Using your own software
- Implement features no other piece of software has
- Design software according to own needs

„Because I can“

- Experiment
- Learn
- Freedom to decide
- Software has almost no resource requirements

 **Passion**

Act II: Promotion to a Respected Maintainer



Over time, Alex's project grows. It attracts other developers who want to share their vision and contribute. Alex learns to work with a team, understand the dynamics of management and create an inclusive and respectful community culture. They develop into a "servant leader", a person who puts her team's needs before their own, and learns that maintainership goes far beyond writing code.

What does a maintainer do?

Activities

- Architecture and design of the software
- Strategic decisions on features
- Designing the roadmap
- Responsibility for releases
- Code review
- Management of the code repository
- Managing the rights of other contributors
- Responding to incoming questions, issues, pull requests
- Mentoring of new contributors
- Moderation of discussions
- Ensuring compliance with the Code of Conduct
- Presentations at conferences
- ...

➔ **Reputation**

“Those who do the work, decide”



Call Incoming...

How do maintainers finance their work?

Resources

- Free time, as a hobby (note: this is a privilege!)
- Study time (e.g. during university)

- Working time, freely available (e.g. 20% time)
- Working time, dedicated to open source (e.g. hired as a maintainer)
- Working time, as a regular part of work projects

- Donations
- Crowd sourcing
- Funding (e.g. public funding or research)

Challenges

- Independence
- Motivation (extrinsic vs. intrinsic motivation)
- Administrativa (taxes, etc.)

→ What are the incentives?



But with growth also comes challenges. There is friction between traditional corporate structures and the Open Source community. Alex needs to learn how to mediate between different stakeholders, how to deal with companies that have different expectations and demands, and how to maintain the independence of their project while remaining open to collaboration and partnerships.

Companies vs. Maintainers



Cultural differences

- Status vs. earned reputation
- Closed vs. open

Process differences

- Hierarchy vs. peer production
- Planned production vs. emergent creation

Differences in resources

- “8 to 5” vs. “When I have the time and inclination”
- Project activity vs. life task

Differences in commitment

- Obligation vs. voluntariness
- External regulation vs. personal responsibility

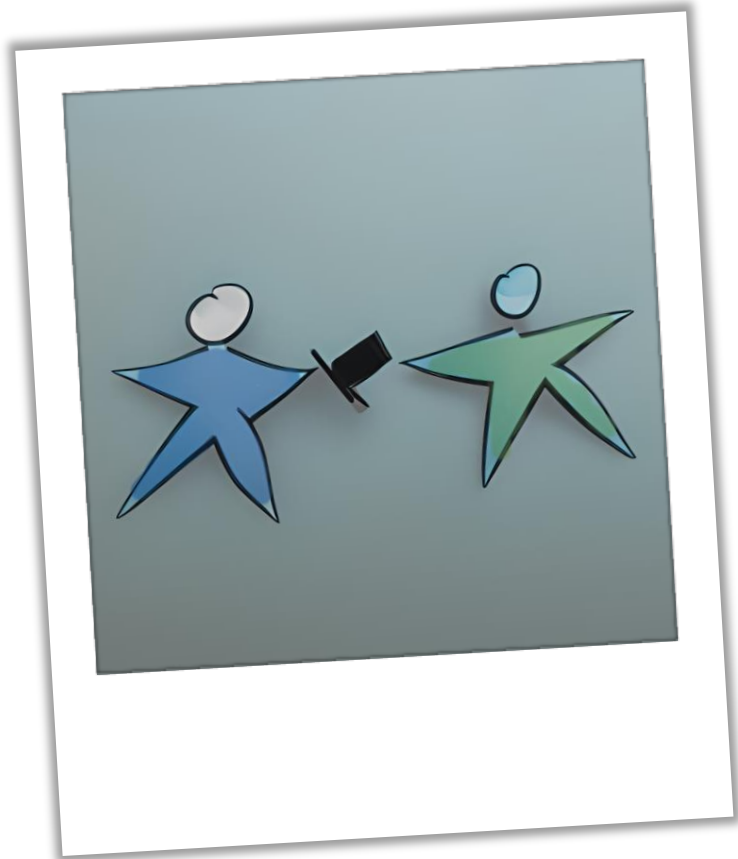
“I’m not a supplier“ aka „Maintainers owe you nothing“

Challenges for companies:

- ➔ Courage to constructive loss of control

Challenges for maintainers:

- ➔ Patience with corporate culture



After many successful years, Alex faces one of the biggest challenges of a maintainer: passing on their role to someone else. They need to find a successor who shares their vision and has the skills to lead the project into the future. It is an emotional yet necessary step to ensure the sustainability of the project.



Alex passes on the Maintainership, but they do so with the certainty that they have created a community based on respect, collaboration and a shared vision. Alex remains a valued member of the community.

Years later, Alex is invited to speak at a conference. With a smile, they share the secret of their success:

“The maintainer is not the boss, but the servant of their community. True leadership lies in this service. Because the true capital of an Open Source project is not in the code, but in the people and the community that keep it alive.”

Maintainers are not all the same

Differences

Motivation

- Development as part of the job
- Scientific work
- Projects managed by companies
- Success can look very different and may not even be desired

Funding

- Voluntary work
- Donations, crowd-sourcing
- Time provided by the employer
- Part of company projects

Governance

- Ad hoc
- Informal but structured
- Foundation

Similarities

- **High sense of responsibility**
- **Autonomous action**
- **Balance of interests**
- **„Servant leader“**



Call Incoming...



Contact

Max Mehl

Open Source Governance & Strategy
DB System GmbH

✉ max.mehl@deutschebahn.com

🐙 [@mxmehl@mastodon.social](https://mstdn.social/@mxmehl)

🐙 [@mxmehl](https://mstdn.social/@mxmehl)



www.dbsystem.de