Sovereign Tech Fund

Apache Log4j trifft Sovereign Tech Fund

27. September 2024: JUG Saxony Day

Hey there!

Mirko Swillus

Program Manager
Sovereign Tech Fund

Christian Grobmeier

VP Data Privacy
Apache Software Foundation

Agenda

Vorstellung

→ Christian und die Apache Software Foundation

→ Mirko und der Sovereign Tech Fund

Interview

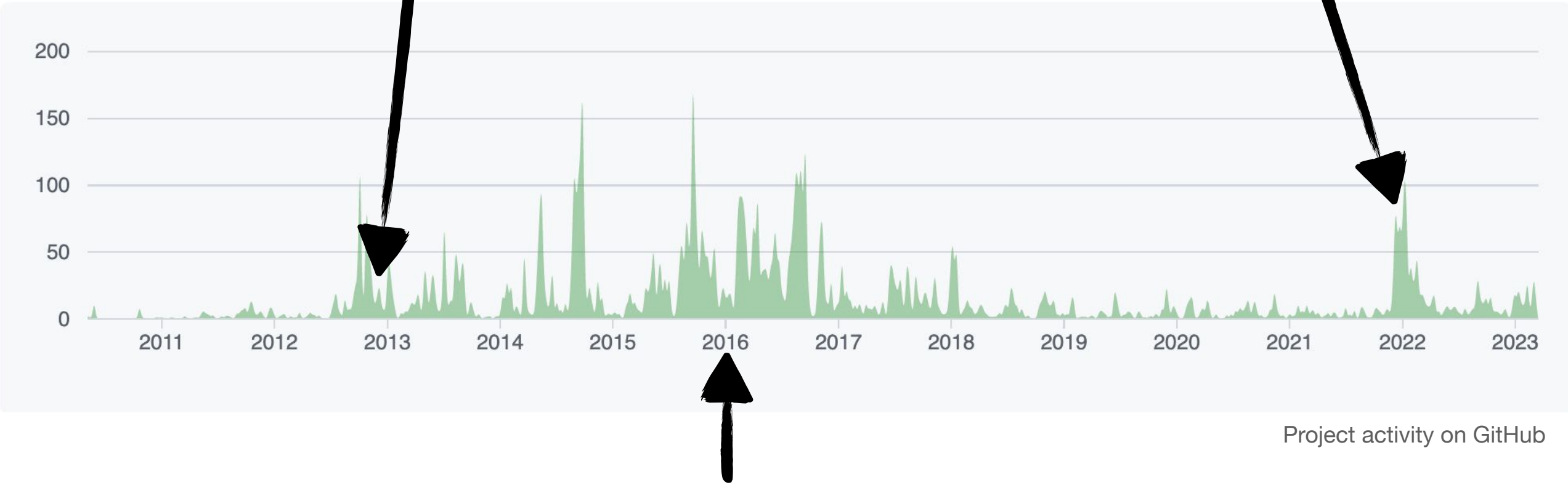
→ Lagerfeuergeschichten und mehr

Eure Fragen!

Christian & Apache log4j

log4shell was born

log4shell was found



Project activity on GitHub

Blackhat Conf on JNDI Injection

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 ..

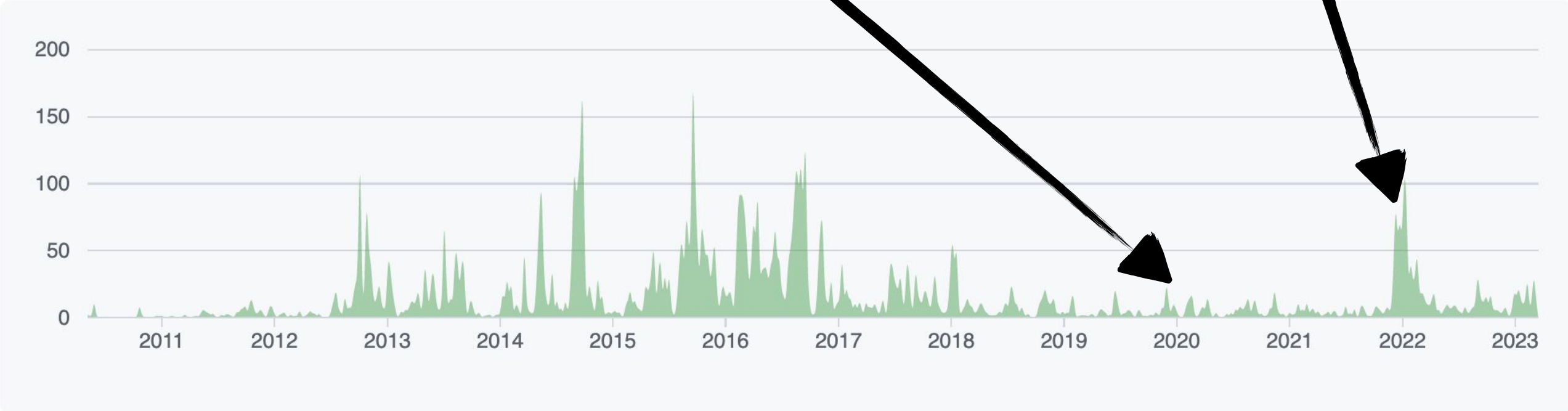
The Log4j Team
DESTROYED MY WEEKEND!!!

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.

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

log4j Latest Statistics

158,811,270

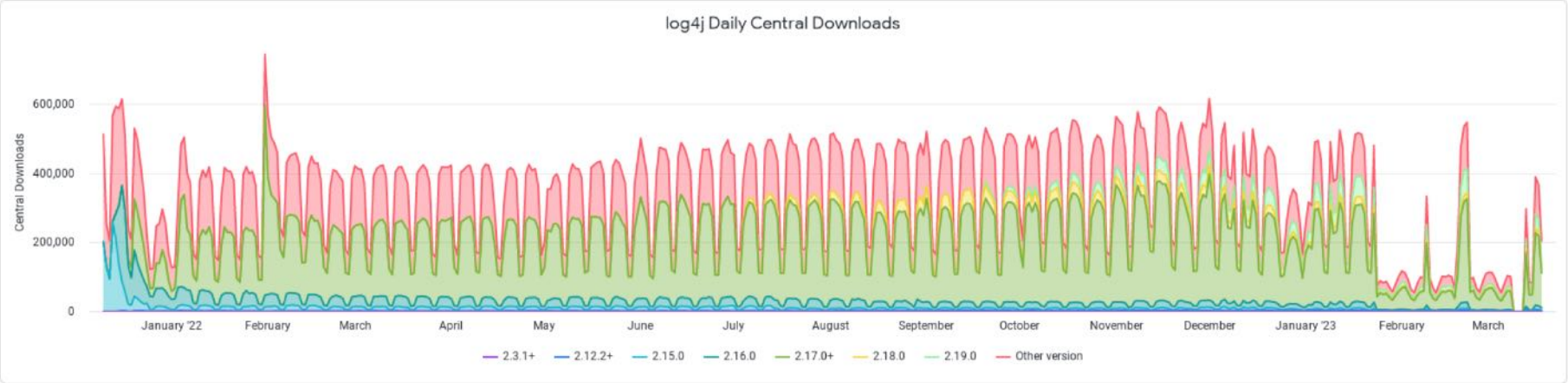
Total Downloads Since Dec 10, 2021

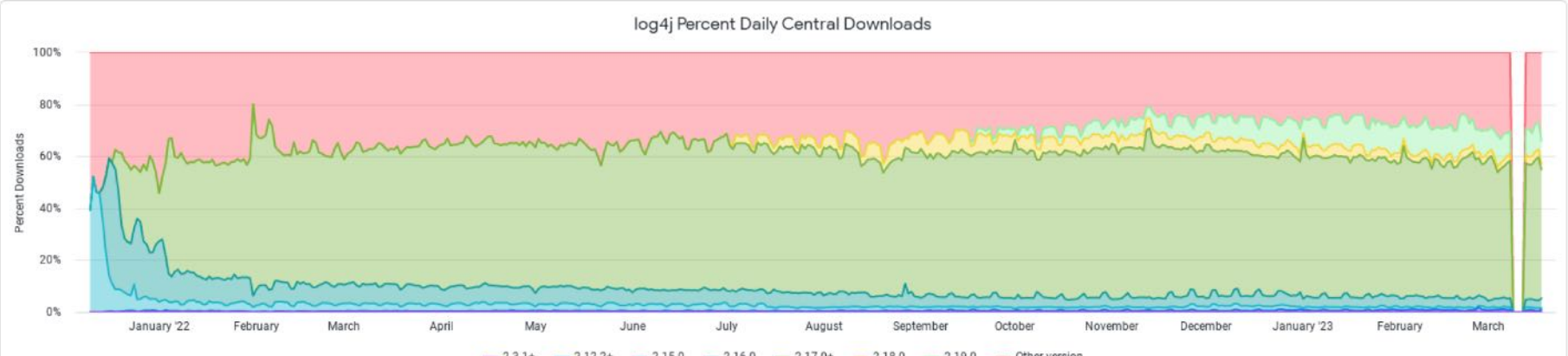
33 % vulnerable

34 %

Vulnerable Downloads Last 24 Hours

203,707 total downloads





Screenshot from 20.03.2023.

34% of daily downloads use vulnerable versions

Mirko & Sovereign Tech Fund

Picard Tips

· 13h

Picard engineering tip: Maintenance of existing systems is just as important as building new capabilities.

9 252 82

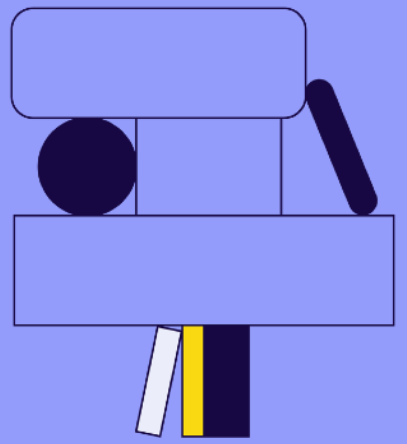
March 18, 2024 at 20:13 ·


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SUPPORTED BY A RANDOM PERSON IN NEBRASKA WHO HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

„As the world blazes ahead into a modern age of startups, code and technology, infrastructure continues to lag behind.
The **cracks** in the foundation are not obvious right now, but they **are widening**“

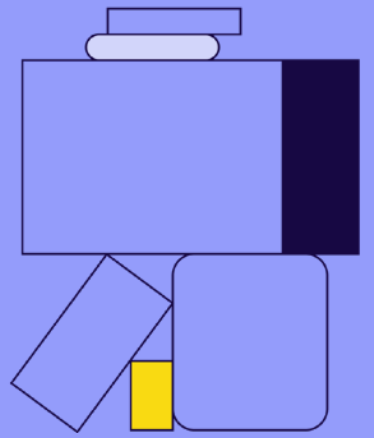
-Nadia Asparouhova, **Roads and Bridges**

Unsere Ziele



Wir arbeiten an einer nachhaltigen Stärkung des Open-Source-Ökosystems. Wir konzentrieren uns auf Sicherheit, Stabilität, technologische Vielfalt und die Menschen hinter dem Code.

Programme



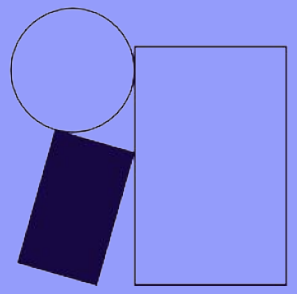
- General Fund
- Bug Resilience Program
- Challenges
- Neu (frisch seit letzter Woche!) :
  Fellowship for Maintainers (Pilot 2025)

Case Study
Log4j

Investment: € 596,160.00

Investment Years: 2023, 2024

logging.apache.org/log4j

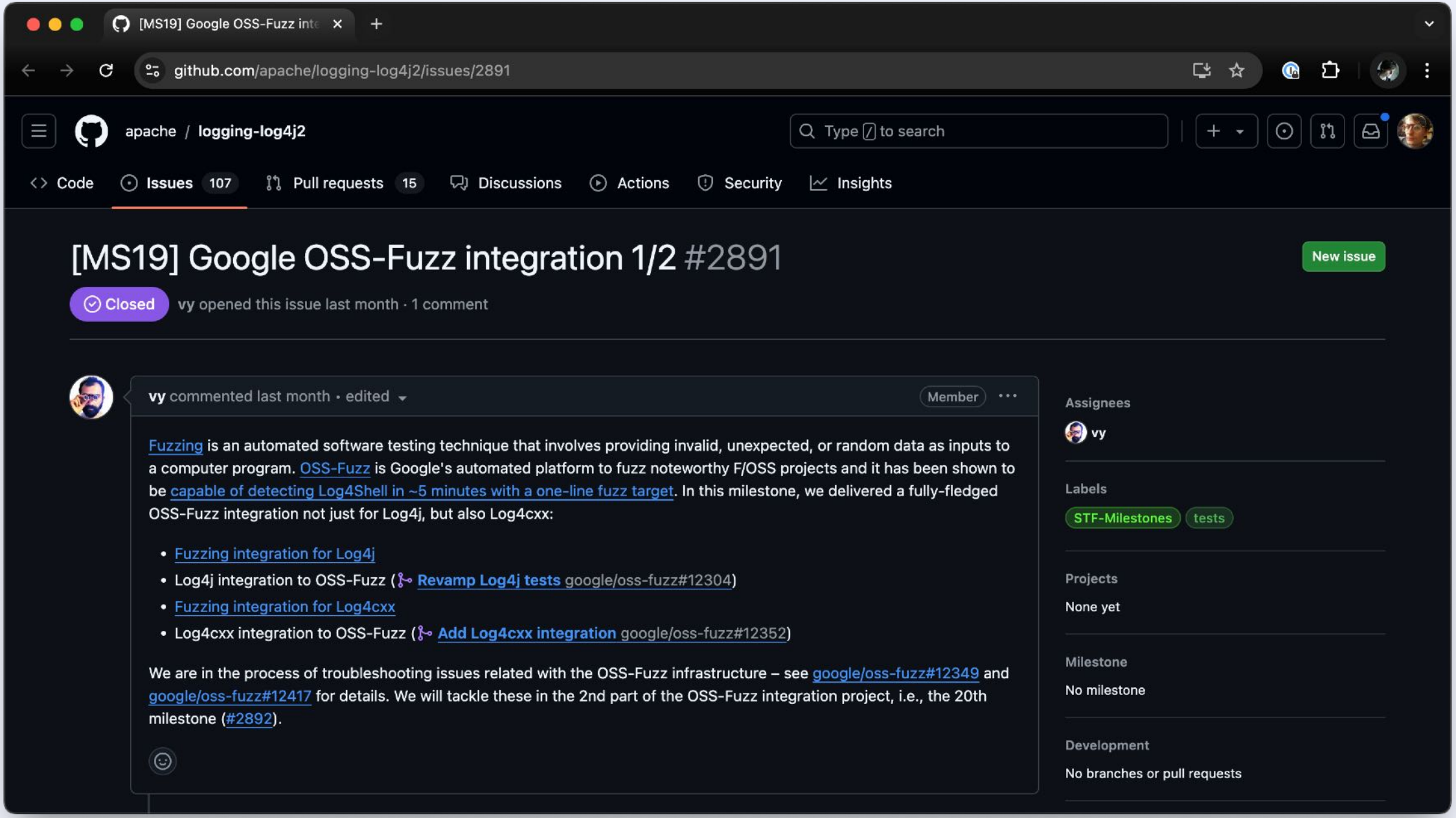


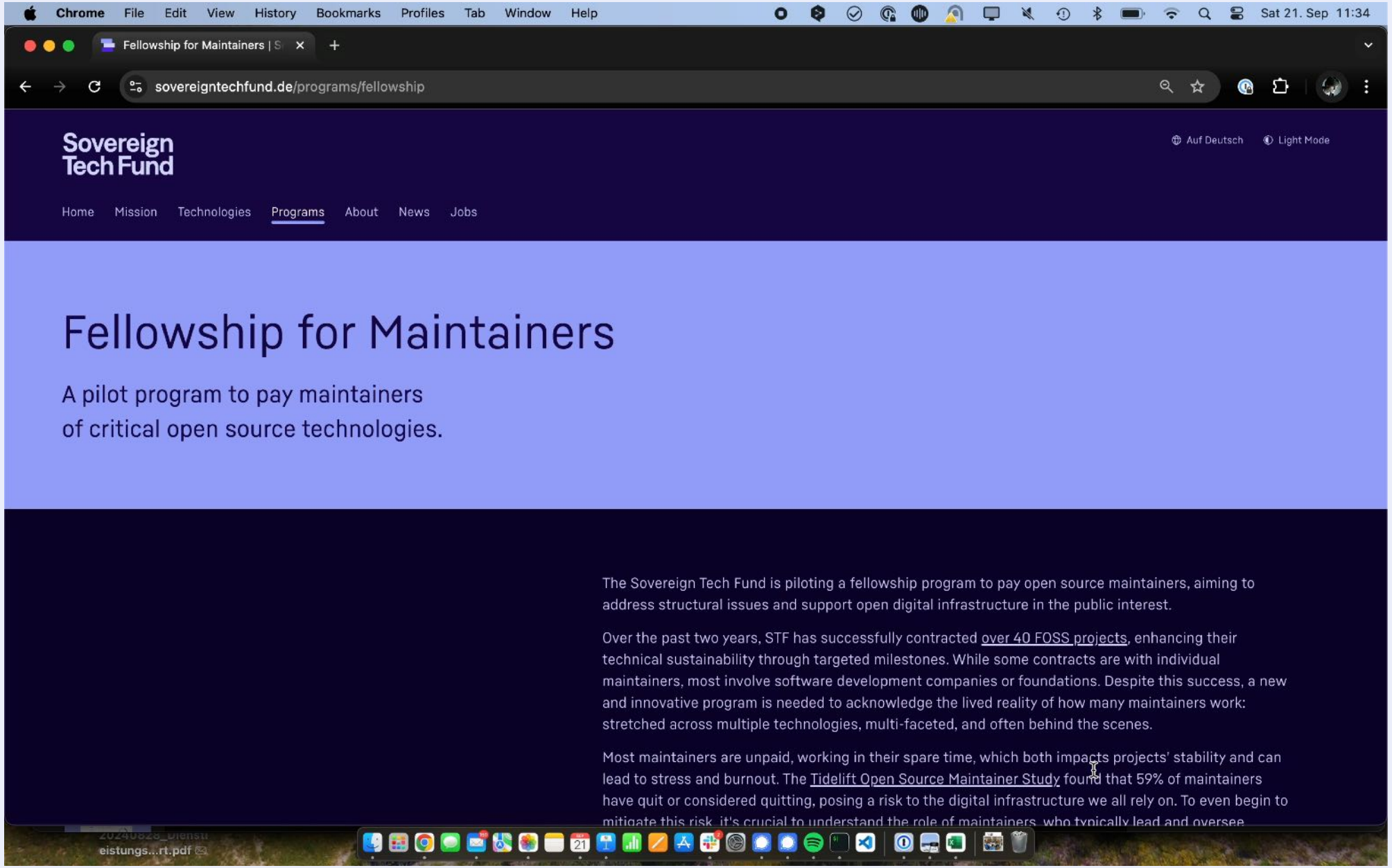
Improving security, stability and trust in Java logging

Objective: To upgrade the Log4j project infrastructure and improve security protocols

Outcomes: new release pipeline for vulnerability responses, fuzz testing for early detection, and SBOMs for better dependency tracking.

Why It Matters: Log4j is a foundational component and its vulnerabilities can have far-reaching consequences.


[MS19] Google OSS-Fuzz inte
github.com/apache/logging-log4j2/issues/2891
apache / logging-log4j2
Type / to search
Code
Issues 107
Pull requests 15
Discussions
Actions
Security
Insights
[MS19] Google OSS-Fuzz integration 1/2 #2891
New issue
Closed
vy opened this issue last month · 1 comment
vy commented last month • edited
Member
Fuzzing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. OSS-Fuzz is Google's automated platform to fuzz noteworthy F/OSS projects and it has been shown to be capable of detecting Log4Shell in ~5 minutes with a one-line fuzz target. In this milestone, we delivered a fully-fledged OSS-Fuzz integration not just for Log4j, but also Log4cxx:
Fuzzing integration for Log4j
Log4j integration to OSS-Fuzz (Revamp Log4j tests google/oss-fuzz#12304)
Fuzzing integration for Log4cxx
Log4cxx integration to OSS-Fuzz (Add Log4cxx integration google/oss-fuzz#12352)
We are in the process of troubleshooting issues related with the OSS-Fuzz infrastructure – see google/oss-fuzz#12349 and google/oss-fuzz#12417 for details. We will tackle these in the 2nd part of the OSS-Fuzz integration project, i.e., the 20th milestone (#2892).
Assignees
vy
Labels
STF-Milestones
tests
Projects
None yet
Milestone
No milestone
Development
No branches or pull requests


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Sat 21. Sep 11:34
Fellowship for Maintainers | S
sovereigntechfund.de/programs/fellowship
Sovereign Tech Fund
Auf Deutsch
Light Mode
Home Mission Technologies Programs About News Jobs
Fellowship for Maintainers
A pilot program to pay maintainers of critical open source technologies.
The Sovereign Tech Fund is piloting a fellowship program to pay open source maintainers, aiming to address structural issues and support open digital infrastructure in the public interest.
Over the past two years, STF has successfully contracted over 40 FOSS projects, enhancing their technical sustainability through targeted milestones. While some contracts are with individual maintainers, most involve software development companies or foundations. Despite this success, a new and innovative program is needed to acknowledge the lived reality of how many maintainers work: stretched across multiple technologies, multi-faceted, and often behind the scenes.
Most maintainers are unpaid, working in their spare time, which both impacts projects' stability and can lead to stress and burnout. The Tidelift Open Source Maintainer Study found that 59% of maintainers have quit or considered quitting, posing a risk to the digital infrastructure we all rely on. To even begin to mitigate this risk, it's crucial to understand the role of maintainers, who typically lead and oversee
eistungs...rt.pdf


open
source
people
think
maintainers
companies
work
thank
fellowship
help
many
needs
support
funding
community
great
paid
lot
time
really
get
need
well
give
currently
actually
paying
might
may
ways
foss
initiative
thanks
idea
oss
general
free
maintainer
security
something
much
fund
public
tech
contribute
new
stf
money

8 Hours Sleep & Relax

Thank you!

Connect with Christian:

Mastodon: mastodon.social/@grobmeier
LinkedIn: https://www.linkedin.com/in/grobmeier/
Web: https://grobmeier.solutions
Email: cg@grobmeier.de

Sovereign Tech Fund

Learn more about us: www.sovereigntechfund.de

Say Hello: info@sovereigntechfund.de