Open & Secure

Nikita Tripathi
Software Engineer / Graphic Designer
nekonya3@fedoraproject.org

The most transparent code in the world can hide the most dangerous vulnerabilities

nekonya3@fedoraproject.org

Roadmap

- Demystifying the "Free Stuff”
- The Many Eyeballs Hypothesis
- The Closed Source Illusion
- Log4Shell : The Wake-Up Call
- Managing Security

Chapter 1

Demystifying The “Free Stuff”

nekonya3@fedoraproject.org

What Open Source Really Means

The Four Freedoms

Use

Modify

Redistribute

Distribute

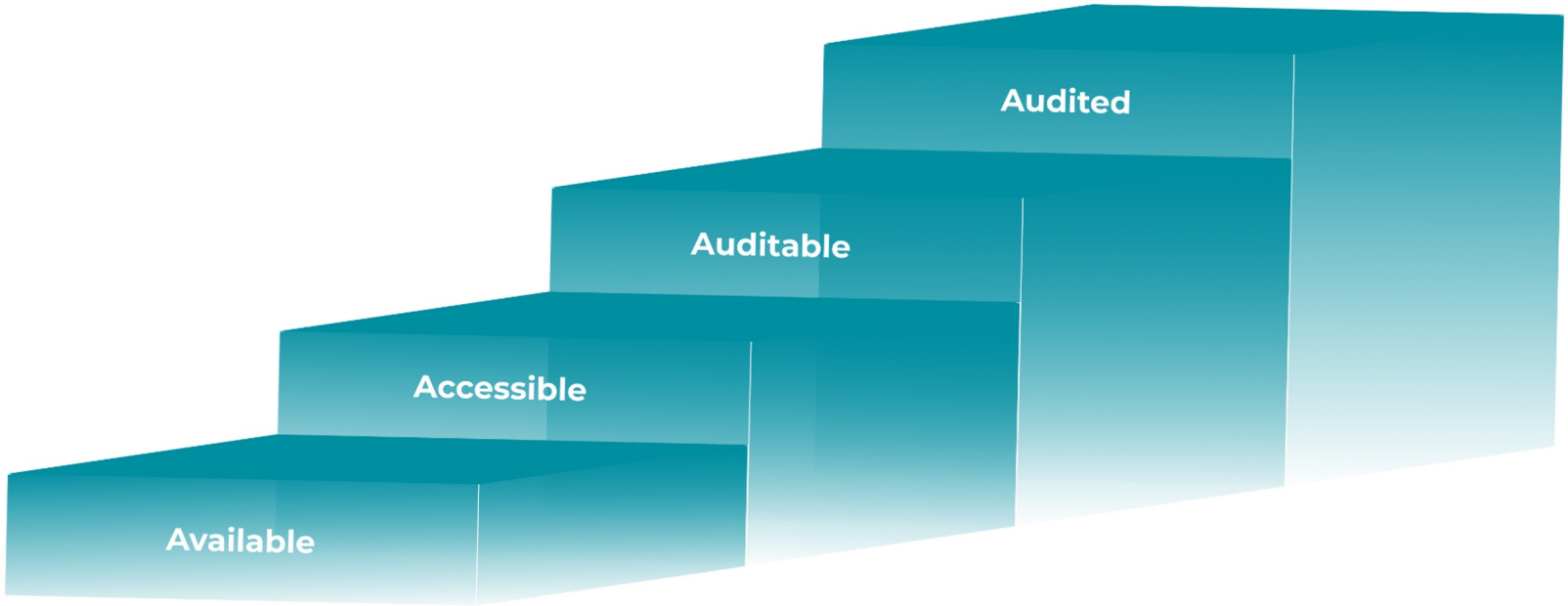
nekonya3@fedoraproject.org

Free software costs Nothing.

nekonya3@fedoraproject.org

Transparency Spectrum

Most open source sits at Level 1-2



nekonya3@fedoraproject.org

The “Jenga Tower” Problem

Supply Chain reality and the Dependency Explosion

THE LINUX FOUNDATION | Europe

JOIN

Home / Blog / The Rising Threat of Software Supply Chain Attacks: Managing Dependencies of Open Source projects

11 MIN READ

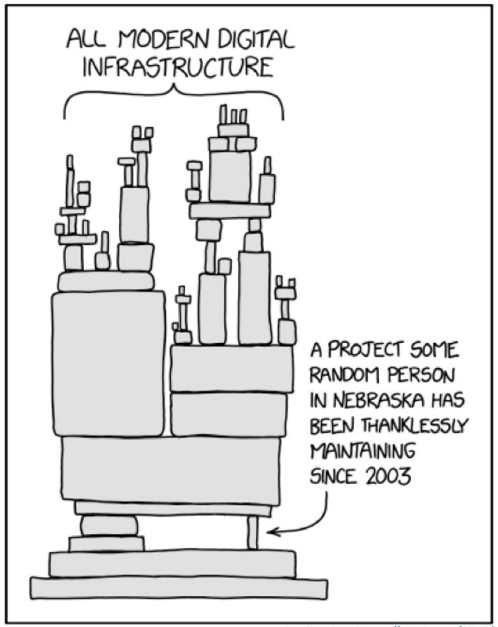
The Rising Threat of Software Supply Chain Attacks: Managing Dependencies of Open Source projects

PAOLO MAINARDI | 15 AUGUST 2023

Open source is flourishing like never before. It is estimated that at least 90% of companies use it, and based on a report by Synposys in 2022, 97% of commercial codebases utilize open source components.

Today, open source represents a significant competitive advantage and opportunity in all sectors where it is applied. It allows anyone to build products by assembling, remixing, and reusing existing modules, libraries, and tools instead of building everything from scratch. This means faster progress, accelerated time-to-market, and a more competitive industry space for everyone involved by adopting common standards.

As per a report, around 70% to 90% of a contemporary application "stack" comprises pre-existing OSS. Though it provides flexibility, it also comes with a cost.



Attribution: https://xkcd.com/2347/

nekonya3@fedoraproject.org

Chapter 2

The Many Eyeballs Hypothesis

Linus's Law Deep Dive

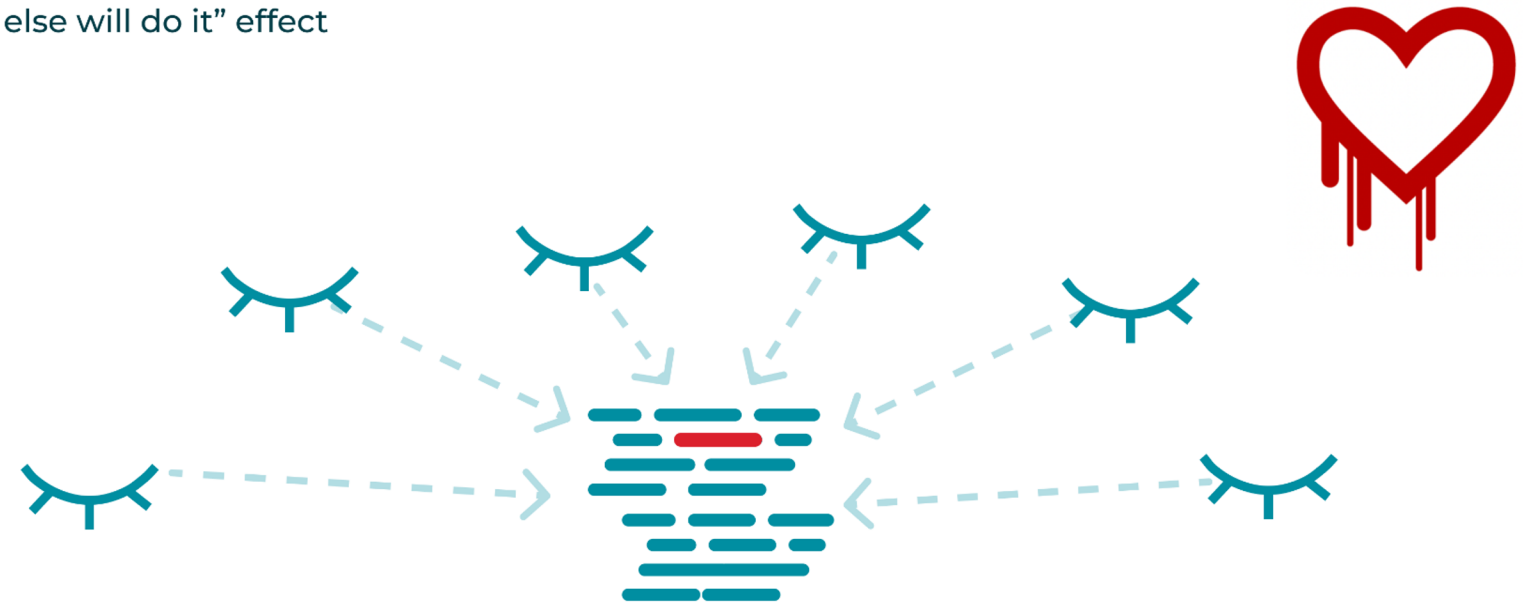
"Given enough eyeballs, all bugs are shallow"

27 Million lines of code

nekonya3@fedoraproject.org

The Downside

“Someone else will do it” effect



27 Million lines of code

nekonya3@fedoraproject.org

Modern Trends

- Reduction in CVE disclosure time from 200 days to 90 days
- HackerOne reports 400% increase in valid submissions
- **GitHub** Security Advisories:
  - 50,000+ vulnerabilities disclosed in 2023
  - Dependabot scanning 40 Million repositories
  - 70% of vulnerabilities reported by external researchers
- **Linux Kernel** exploits are rare and quickly patched

Chapter 3

The Closed Source Illusion

Obscurity

nekonya3@fedoraproject.org

Obscurity

nekonya3@fedoraproject.org

“The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards, and even then I have my doubts”

-Gene Spafford

nekonya3@fedoraproject.org

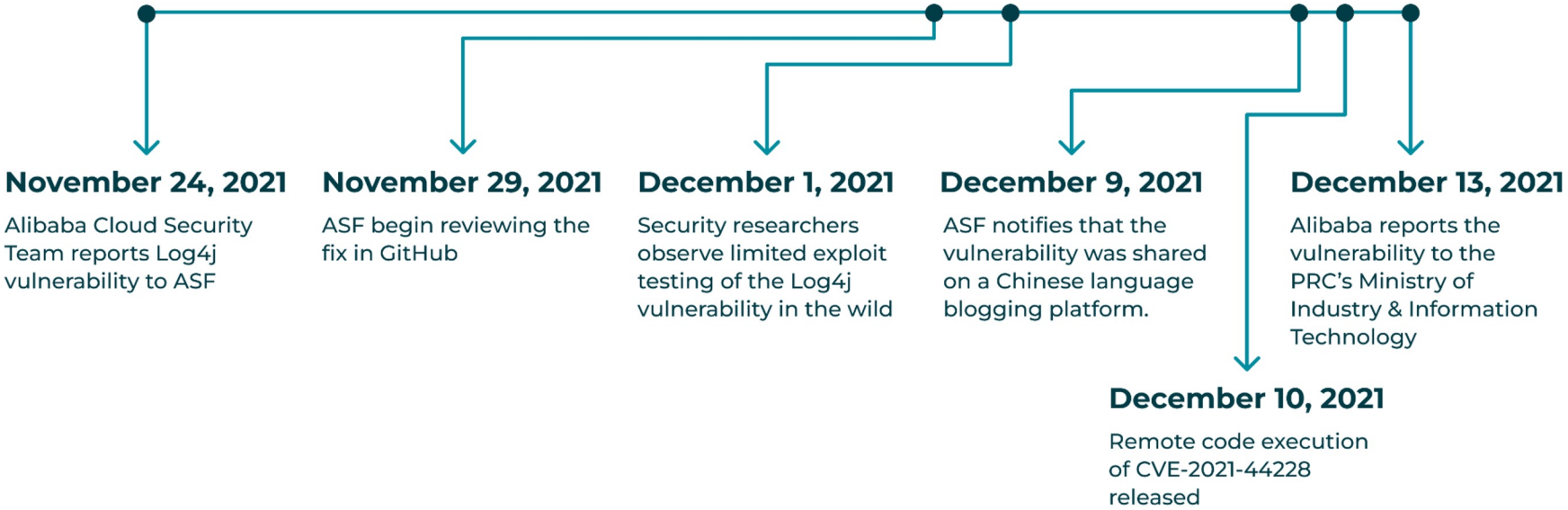
Kerckhoffs's Principle

nekonya3@fedoraproject.org

Chapter 4

Log4Shell
The Wake-Up Call

Timeline



nekonya3@fedoraproject.org

The Impact

China Suspends Partnership with Alibaba Cloud for Log4Shell Vulnerability

China government suspends partnership with Alibaba Cloud for not sharing details of Log4Shell.

Admin Updated: December 23, 2021 · 1 min read

Tweet Share Add as preferred source

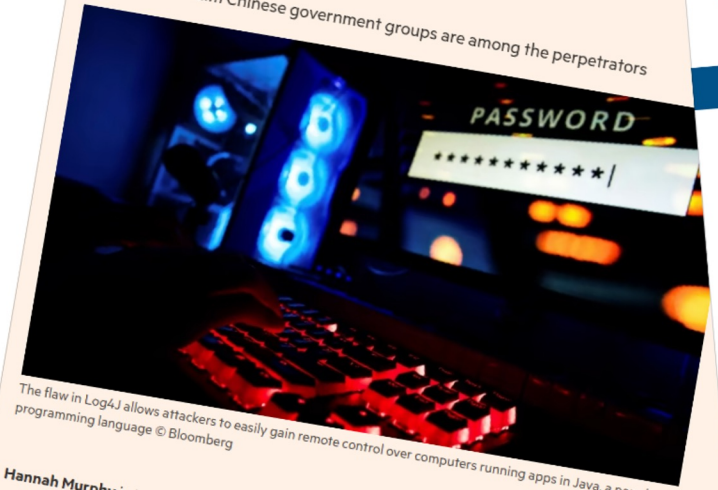
FINANCIAL TIMES

US COMPANIES TECH MARKETS CLIMATE OPINION LEX WORK & CAREERS LIFE & ARTS HTSI

Cyber Security + Add to myFT

Hackers launch more than 1.2m attacks through Log4J flaw

Researchers claim Chinese government groups are among the perpetrators



The flaw in Log4J allows attackers to easily gain remote control over computers running apps in Java, a popular programming language © Bloomberg

Hannah Murphy in London

Published DEC 14 2021 | Updated DEC 14 2021, 21:16

CISA CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics Spotlight Resources & Tools News & Events Careers About

Home / News & Events / News / Statement from CISA Director Easterly on "Log4j" Vulnerability

PRESS RELEASE

Statement from CISA Director Easterly on "Log4j" Vulnerability

Released: December 11, 2021

Revised: December 11, 2021

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, CYBER THREATS AND ADVISORIES, INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN SECURITY

nekonya3@fedoraproject.org

Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly released the following statement today on the "log4

Technical Dive

Ubiquity

Invisible Dependencies

Feature Creep

Maintenance Imbalance

nekonya3@fedoraproject.org

Lessons Learned

Positive Outcomes:

1. SBOM Acceleration
2. Supply Chain visibility tools
3. Incident Response improvements
4. Industry Collaboration

Systemic Issues Revealed:

1. Sustainability Crisis
2. Dependency Hell
3. Security Assumptions

nekonya3@fedoraproject.org

Chapter 5

Open Source Security Today

Existing Challenges

1. Sustainability Crisis
2. Skills and Expertise gaps
3. Training and Mentorship challenges
4. Supply Chain coordination issues
5. Legacy System integration challenges

nekonya3@fedoraproject.org

Emerging Challenges

1. AI-Generated code risks
2. ML Model security
3. Cloud-Native Security Complexity
4. Edge Computing challenges
5. IoT-specific issues

nekonya3@fedoraproject.org

Practical Recommendations

- Inventory
- SBOMs
- ID components
- Dependency approvals

- Scans in CI/CD
- Automated alerts
- Dependency update tests
- Code securely

- Review board
- Escalations
- Compliance workflows
- Training

nekonya3@fedoraproject.org

Security is only as strong as your commitment to managing it

nekonya3@fedoraproject.org

Open & Secure

Nikita Tripathi
Software Engineer / Graphic Designer
nekonya3@fedoraproject.org

Appendix

Apache Struts (CVE-2024-5367)

The flaw lies in Struts' file upload mechanism; Attackers can manipulate file upload parameters to enable path traversal, allowing them to place malicious files into otherwise restricted directories. Under certain conditions, this can lead to remote code execution, enabling unauthorized actors to run arbitrary code, exfiltrate sensitive data, or compromise entire systems

nekonya3@fedoraproject.org

Heartbleed Bug (OpenSSL)

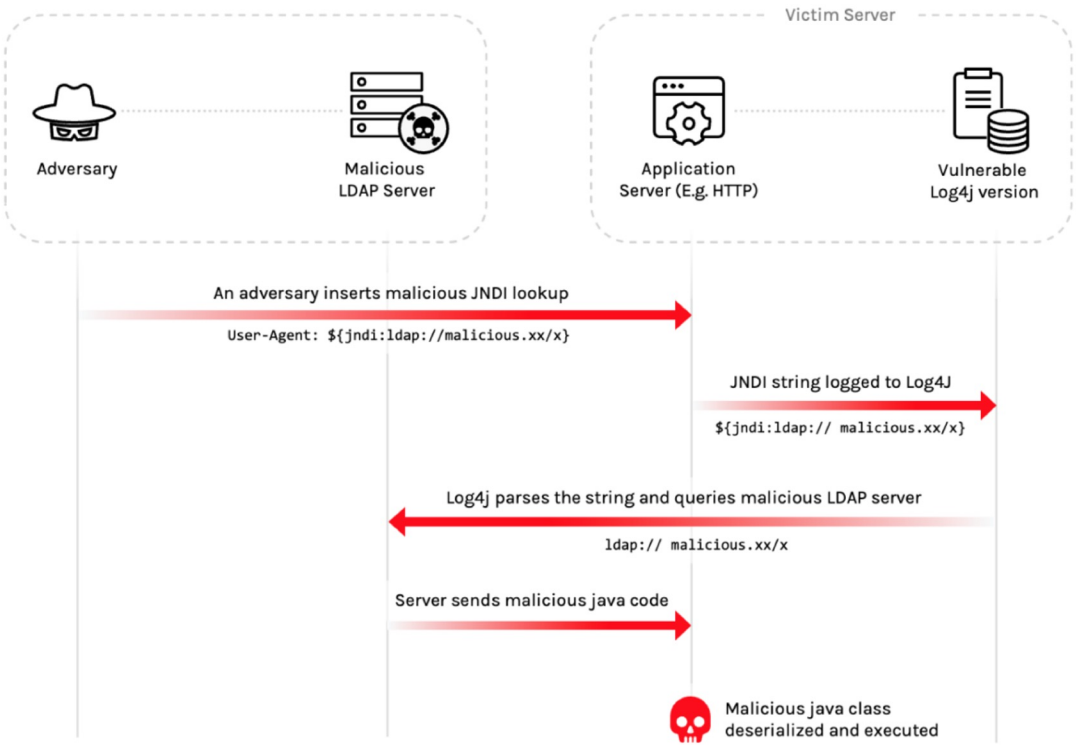
Heartbleed happened due to a missing bounds check in the OpenSSL library's implementation of the TLS heartbeat extension. An attacker could send a heartbeat request that falsely claimed a much larger payload size than the data actually sent. The server would then allocate memory for the large size, copy the smaller actual payload, and return the entire block of memory, which included sensitive information like private keys and passwords, along with the payload

Log4Shell (CVE-2021-44228)

Log4Shell occurred due to an "improper input validation" in the **Java Naming and Directory Interface** (JNDI) lookup feature of Apache's Log4j logging library. This flaw allowed attackers to send a crafted string in a log message that would cause the application to connect to a malicious server, download, and execute arbitrary code.

nekonya3@fedoraproject.org

Log4Shell (CVE-2021-44228)



Attribution: https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/log4j-vulnerability/

nekonya3@fedoraproject.org