

Managing Open Source Software Supply Chains

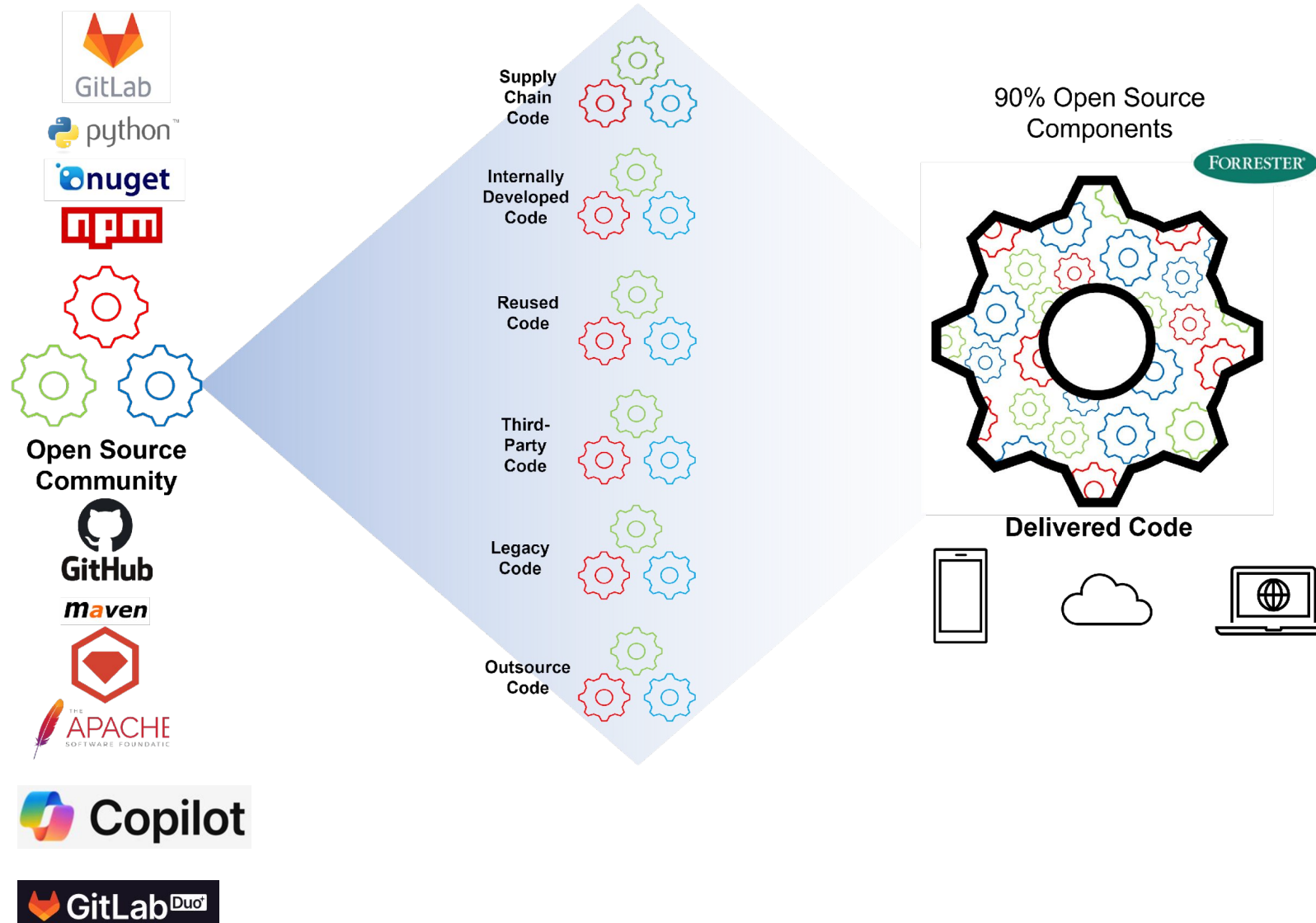
```
mirror_mod = modifier_ob.modifiers[0]
# Set mirror object to mirror_mod
mirror_mod.mirror_object = mirror_ob

if operation == "MIRROR_X":
    mirror_mod.use_x = True
    mirror_mod.use_y = False
    mirror_mod.use_z = False
elif operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add
mirror_ob.select= 1
modifier_ob.select=1
context.scene.objects.active = mirror_ob
print("Selected" + str(modifier_ob.name))
mirror_ob.select = 0
one = bpy.context.selected_objects[0]
data.objects[one.name].select = 1
print("please select exactly one object")

--- OPERATOR CLASSES ---
```

Software Supply Chain



The Log4j Vulnerability

- Log4j, Apache logging framework
- Found everywhere from big corps to SMB's
- Easily exploited to take control of vulnerable systems remotely
- Hackers actively scanning the internet for affected systems
- Within 72 hours 100 attacks a minute
- Tools developed that automatically attempt to exploit the bug
- How widespread is the problem?

"The Log4j meltdown speaks more to how widely the effects of a single flaw can be felt if it sits in a foundational piece of code that is incorporated into a lot of software" – WIRED December 12, 2021

<https://www.wired.com/story/log4j-flaw-hacking-internet/>

THE BARRAGE —


Hackers launch over 840,000 attacks through Log4J flaw

Researchers claim Chinese government groups are among the perpetrators.

HANNAH MURPHY, FINANCIAL TIMES - 12/14/2021, 3:32 PM

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

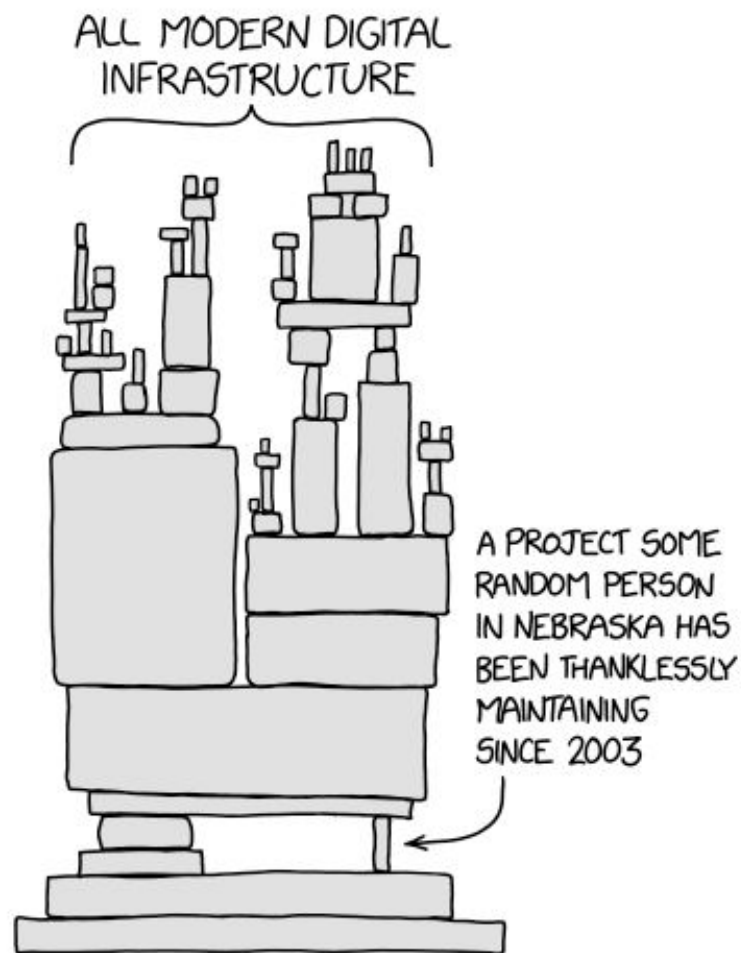
 NIST: NVD **Base Score:** 10.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

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.

CVE-2021-44228 – NVD “Critical” Rating of 10/10

The sad truth



<https://imgs.xkcd.com/comics/dependency.png>



The human toll of log4j maintenance

<https://dev.to/yawaramin/the-human-toll-of-log4j-maintenance-35ap>



Source Code Control
Open Source Risk Management Specialists

Increase in legal challenges.

- Increase in license enforcement
 - Ghostscript
 - iText
- License changes
 - Elastic
 - Kabana
 - Hashicorp
 - MongoDB
- Increase in legal cases
 - Software Freedom Conservancy

Tesla inches toward GPL compliance in low gear: Source code forcibly ejected into public

Some software blueprints doled out after years of complaints

By Thomas Claburn in San Francisco



Important Open Source Ruling Confirms Enforceability of Dual-Licensing and Breach of GPL for Failing to Distribute Source Code

By Hean L. Koo and James Gatto on May 15, 2017

Posted in [Gaming](#), [Intellectual Property](#), [Social Media](#), [Transactions](#)



EIN PRESSWIRE

**Artifex S
Copyright
Siemens
Software**

SOFTWARE FREEDOM CONSERVANCY SUES VIZIO OVER SOURCE CODE

New York-based nonprofit Software Freedom Conservancy (SFC) has sued television manufacturer Vizio Inc to force it to share the source code for the software used in its smart TVs.



External forces driving forcing risk control

MANDATES



US Cyber Executive Order 14028
(May 2021)

EU Cyber Resiliency Act
(September 2022)

There are many other industries and countries...

Healthcare (FDA) | Auto (NHTSA) | Energy (NERC) | Consumer (FTC)

Multiple EU Agencies (Cloud, IoT, Medical, Payments, Telco)

Example: FDA Cybersecurity Modernization Action Plan (CMAP)



PROCESS



ISO/IEC 5230:2020
ISO/IEC DIS 18974

OpenChain v2.1 is the International Standard for OSS license compliance

OpenChain Security Assurance Specification v1.1 defines key requirements for a quality OSS security assurance program

FORMAT



SPDX v2.3 is an open standard for communicating Software Bill of Materials (SBOM) information

Coming up: v3.0 (RC published May 8th)



CycloneDX v1.4 is a full-stack Bill of Materials (BOM) standard that provides advanced supply chain capabilities for cyber risk reduction.

Coming up: v1.5 (2023) & v1.6 (2024)



Source Code Control
Open Source Risk Management Specialists

European Regulations

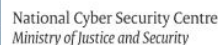
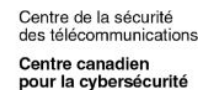
Common themes in latest regulations

- Transparency in the use of third-party open source components
- Software Bill of Materials SBOM mandatory
- Process for remediation mandatory
- **Fines EUR 5-15m or 1-2.5% of the worldwide turnover**

*Manufacturers shall, upon identifying a vulnerability in a component, including in an **open source component**, which is*

- One key thing to note is the call for **cybersecurity liability**: in other words, holding software providers responsible:
 - One angle is limiting organizations from **disclaiming all liability** in EULAs (End-User License Agreements)
 - The other is **duty of care**: in other words, can you demonstrate that you have followed reasonable / industry accepted standards to build secure applications
- To avoid potential **product liability** problems, the cadence of security testing may have to change

third parties



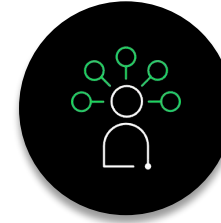
Common Pitfalls



SCA TOOL IS THE
SILVER BULLET



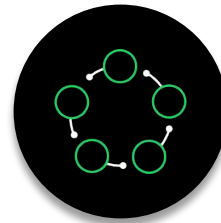
NO CLEAR
PURPOSE



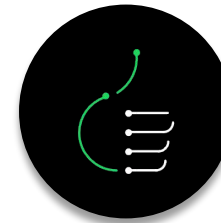
LACK OF CONSISTENT
KNOWLEDGE



NO DEFINED ROLES
AND RESPONSIBILITIES



LACK OF POLICY
AND PROCESS



LACK OF EXECUTIVE
SPONSORSHIP



Source Code Control
Open Source Risk Management Specialists

Interneuron

- Open Source Health Tech Company
- Implemented managing their use of open source from the early stages of the company
- Focus was security and compliance
- Eventually conforming with ISO 5230 and ISO 18974 OpenChain
- Key benefit demonstrating quality of their software development
- Competitive Edge

OPENCHAIN CASE STUDY

How OpenChain Supports Interneuron



ORGANIZATIONS:	CHALLENGES:	SOLUTION:	BENEFITS:
<ul style="list-style-type: none">Community Interest Company (CIC) – a Not for profitfocused on building, developing, and deploying software specifically for the healthcare IT industryEverything developed by Interneuron will be open source and is specified in their articles of association	<ul style="list-style-type: none">Overcoming perception that traditional proprietary software is the least risky optionEnable 100% transparency of the use of third party open sourceDecrease the knowledge gap around measuring open source quality and effectiveness including IP and security vulnerability management in a clinical environment	<ul style="list-style-type: none">Building oversight and governance by designEmpowering and motivating developers to be responsible for complying with company guidelinesEducation – Company wide knowledge sharing of controlled used of open source<ul style="list-style-type: none">Ensure license obligations are metIP is respectedSecure by designUnderpinned by a managed service from OpenChain Partner Source Code Control	<ul style="list-style-type: none">Transparent demonstration of quality assurance; unachievable by proprietary solutionsAutomated tracking third party open source software components for both licensing and security vulnerabilitiesDecreased patent and licensing risksRemove barriers from purchasing decisions, creating competitive advantage and differentiationSecure and compliant by design

<https://openchainproject.org/resources/openchain-case-study-interneuron>

The Interneuron Journey to OpenChain Conformance

Policy

- ✓ What are we managing?

Underpinned by quality data

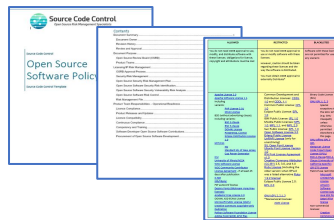
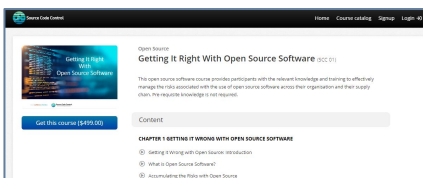
revenera
Code Insight®

Enable self-management

- ✓ Avoid problems in the first place

Independent reporting

- ✓ Management reports



NAME	VERSION	LICENSE	STATUS
angular/animations	10.2.5	MIT	OK
angular/common	10.2.5	MIT	OK
angular/core	10.2.5	MIT	OK
angular/forms	10.2.5	MIT	OK
angular/localize	10.2.5	MIT	OK
angular/platform-browser	10.2.5	MIT	OK
angular/platform-browser-dynamic	10.2.5	MIT	OK
angular/platform-server	10.2.5	MIT	OK
angular/router	10.2.5	MIT	OK
angular/scss	10.2.5	MIT	OK
angular/zone.js	0.11.4	MIT	OK
rxjs	6.6.0	MIT	OK
zone.js	0.11.4	MIT	OK

COMPONENT	VERSION	LICENSE
angular/animations	10.2.5	MIT
angular/common	10.2.5	MIT
angular/core	10.2.5	MIT
angular/forms	10.2.5	MIT
angular/localize	10.2.5	MIT
angular/platform-browser	10.2.5	MIT
angular/platform-browser-dynamic	10.2.5	MIT
angular/platform-server	10.2.5	MIT
angular/router	10.2.5	MIT
angular/scss	10.2.5	MIT
angular/zone.js	0.11.4	MIT
rxjs	6.6.0	MIT
zone.js	0.11.4	MIT



Software Bill of Materials (SBOM)

Questions?

```
mirror_mod = modifier_ob.  
Get mirror object to mirror  
mirror_mod.mirror_object  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True  
selection at the end -add  
mirror_ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier_ob))  
mirror_ob.select = 0  
= bpy.context.selected_object  
data.objects[one.name].select  
print("please select exactly  
-- OPERATOR CLASSES -----
```

