FLEXERA™

COMMON OPEN SOURCE INTAKE ISSUES AND HOW TO RESOLVE THEM

Jeff Luszcz
VP Product Management
jluszcz@flexera.com

@jeffluszcz

Agenda

What is OSS intake

Common Intake flows

What are the problems with the current process?

Types of OSS Intake Issue

Software Vulnerabilities / CVEs

OSS Compliance Issues

Thanks/Q&A

What is OSS Intake?

OSS intake is the process of obtaining Open Source components or code as part of an application you are building

These components can be in source or binary form

This process can be ad hoc or part of a monitored process with strong usage policy

There may be a published License Policy or Workflow

Common Intake flows

Developers Make Requests before usage

Developer selects Component and copies it into codebase

Most Components have Dependencies and Subcomponents

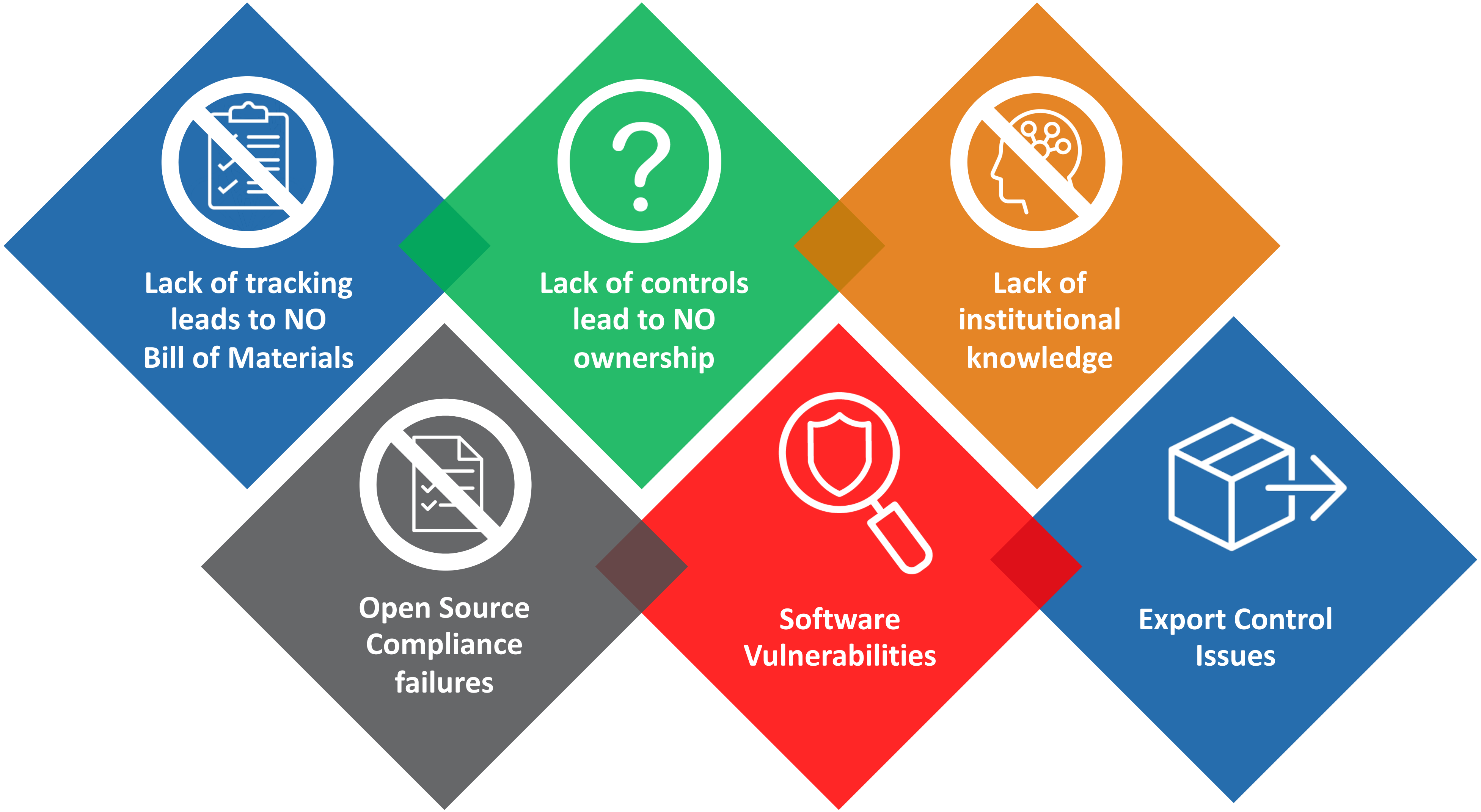
Developer uses a Repository Manager like Maven to pull in component

Repository Manager pulls in Dependencies

Commercial SDKs and libraries and their OSS dependencies

IT selects infrastructure

What are the problems with the current process?



Lack of tracking leads to NO Bill of Materials

Lack of controls lead to NO ownership

Lack of institutional knowledge

Open Source Compliance failures

Software Vulnerabilities

Export Control Issues

Types of OSS Intake Problems

Security Issues:

Software Vulnerabilities / CVEs

Compliance Issues:

OSS License compliance problems

Commercial licensing problems

Patent issues

Export / Encryption issues

Software Vulnerabilities / CVEs

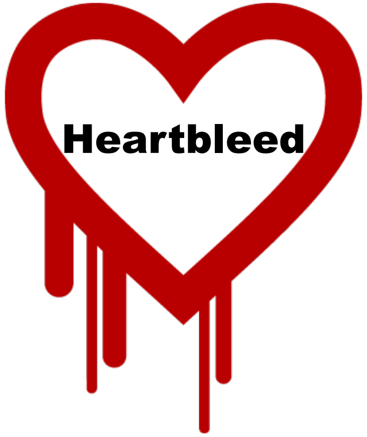
As we saw with Equifax, software vulnerabilities in OSS and other Third Party Software can have serious effects.

The most common remediation is a “simple version” upgrade
(e.g. move from version 1.0 to 1.1)

This can sometimes lead to License Compliance or compatibility issues!

You may also see that you are not affected by the Vulnerability or can resolve with a non-upgrade fix (firewall, remove module, change password)

Software Vulnerabilities / CVEs



CVE-2014-0160

OpenSSL

- 17% of the Internet's secure web servers (500M) believed to be vulnerable to the attack
- Allowed theft of the servers' private keys, users' session cookies and passwords

- **Typical age: 3-4+ years old**

CVE-2014-6271

GNU Bash

- Potentially affects hundreds of millions of computers, servers and devices
- Shellshock can be used to remotely take control of almost any system using Bash

- **Typical age: 5 years old (seen 13 years!)**

CVE-2015-0235

Linux GNU C Library (glibc)

- Affects almost all major Linux distributions
- Millions of servers on the Internet contain this vulnerability

- **Typical age: 3 years**

CVE-2017-5638

Apache Struts2

- Remote Code Execution (RCE) vulnerability in the Jakarta Multipart parser
- Allows attacker to execute malicious commands on the server when uploading files
- Exploits are publicly available, simple to carry out, and reliable

Software Vulnerabilities / CVEs

Customers and Users are checking releases for vulnerabilities with Software Composition Anaylsis (SCA) scan tools

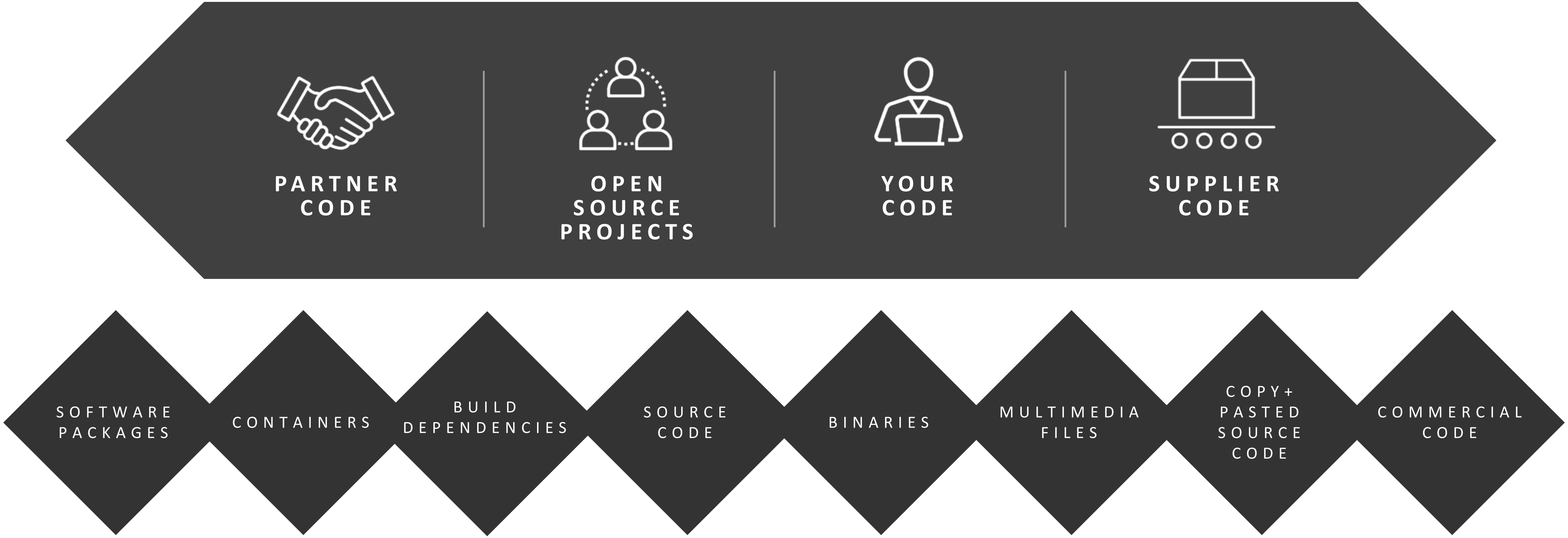
Even if you are NOT affected by the CVE you will likely be asked about it

“We aren’t affected” isn’t always believed, you may need to upgrade anyway

Components don’t get better with age, what was “safe” when selected will likely have vulnerabilities found out over time

You will need to keep checking, even after release

The Software Supply Chain and Remediation



PARTNER CODE

OPEN SOURCE PROJECTS

YOUR CODE

SUPPLIER CODE

SOFTWARE PACKAGES

CONTAINERS

BUILD DEPENDENCIES

SOURCE CODE

BINARIES

MULTIMEDIA FILES

COPY+ PASTED SOURCE CODE

COMMERCIAL CODE

The Software Supply Chain and Remediation

The further back in your supply chain the less likely you are able to get a quick remediation or even an answer to a question

Put pressure on your supply chain to deliver a current Bill of Materials

Put pressure on your supply chain to provide updated for vulnerabilities

You want to build a "Push not Pull" culture with your vendors

Test your supply chain, especially around vulnerabilities

YOU are responsible for everything you deliver!

Intake Issue: Lack of Education and Process

The typical software developer has limited exposure and training regarding Open Source Licensing and Component Usage

The typical company has limited OSS guidance or visible OSS policy

Management and Legal often come in too late to add meaningful help

Problems often are discovered right at ship time

The Remediation process is often opaque or secret due to Legal or Security requirements

Document process, train periodically, make process dynamic

Compliance Issue: GPL Violations

The General Public License requires source code to be distributed to people who receive a work based on that GPLed component

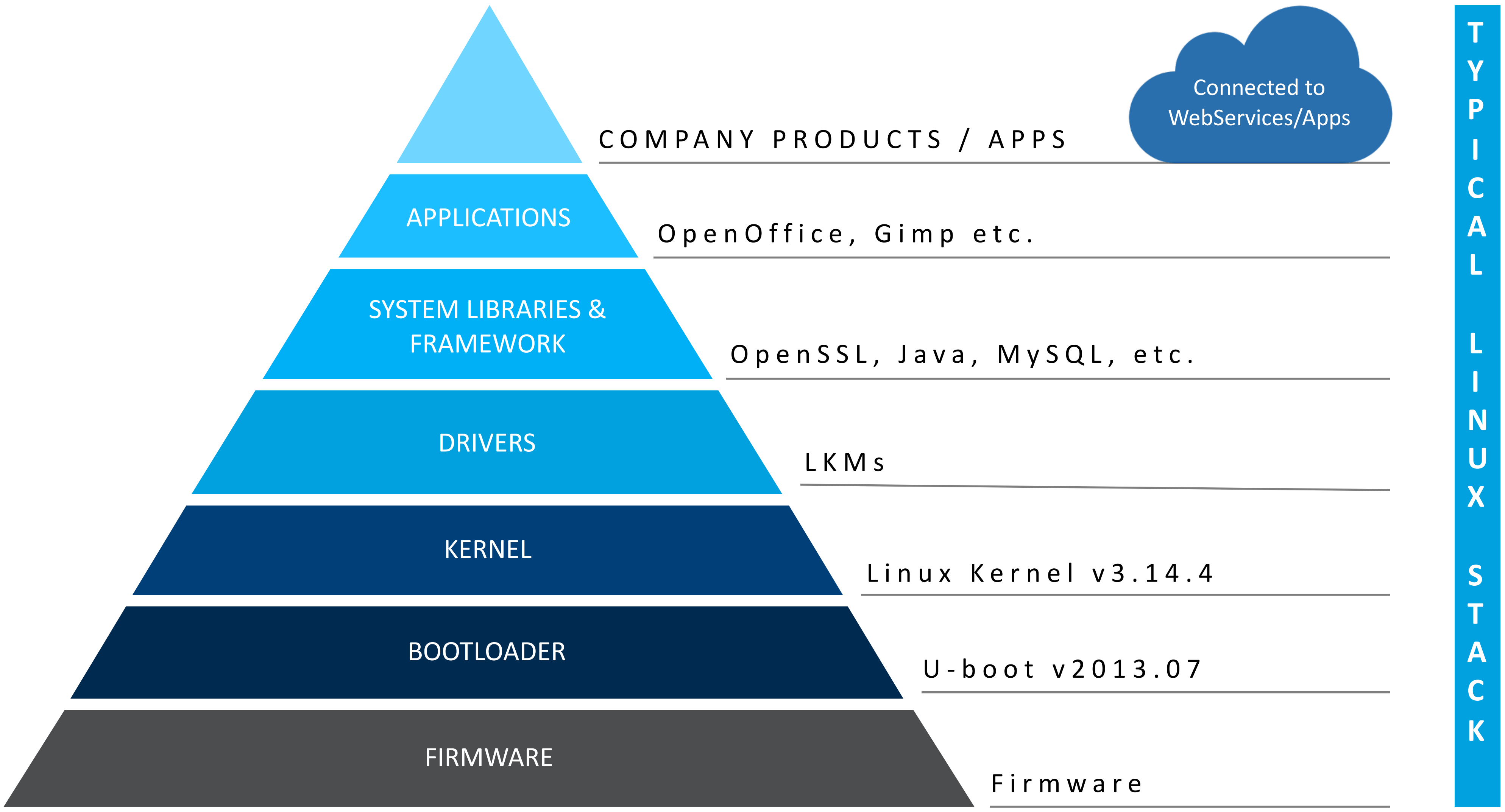
This source code should include everything linked to that component

Common GPL Violations include:

- Not including the GPL license in a release
- Not including source code or written offer for source code

How to fix: Release as open source, Re-architect, Remove component, cleanroom rewrite, relicense (if possible)

Compliance Issue: GPL Policy vs. Software Stack



COMPANY PRODUCTS / APPS

Connected to WebServices/Apps

APPLICATIONS — OpenOffice, Gimp etc.

SYSTEM LIBRARIES & FRAMEWORK — OpenSSL, Java, MySQL, etc.

DRIVERS — LKMs

KERNEL — Linux Kernel v3.14.4

BOOTLOADER — U-boot v2013.07

FIRMWARE — Firmware

TYPICAL LINUX STACK

Compliance Issue: Dual License Violations

It is common to see OSS Components available under multiple licenses

Dual licenses typically telegraph a Business Model or OSS License Model

A common dual license for "Business model" purposes is the option of either a strong Copyleft license OR a Commercial License (e.g. GPL or Commercial or AGPL or Commercial)

Common Examples:

- **Mysql (GPL v2 or Commercial)**
- **iText(AGPL or Commercial)**

How to fix:

- Purchase a Commercial License
- Release product as OSS under the terms of the Copyleft license
- Remove Component

Compliance Issue: Dual License Selection

A common dual license for “OSS license model” purposes is the option of either a strong Copyleft license OR a different license (CDDL or Apache 2.0 or MIT) or a tri-license (MPL or GPL or LGPL)

Common Examples:

Jersey (GPL v2 with Classpath Exception or CDDL 1.1)

How to fix:

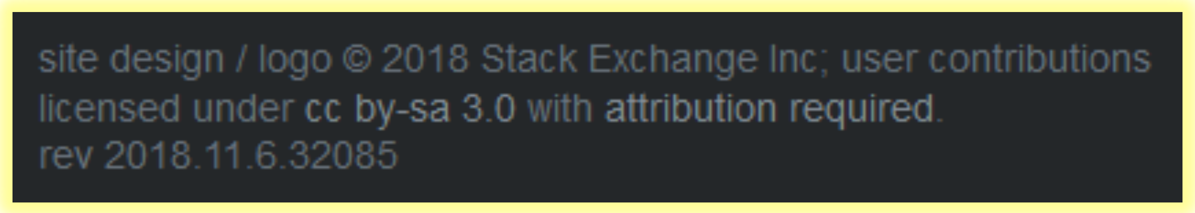
- Select the more “permissive” license, comply with its terms
- Release product as OSS under the terms of the Copyleft license
- Remove Component

Compliance Issue: StackOverflow

StackOverflow is a very popular Q&A forum for programming questions

All user submitted content is licensed under the CC BY-SA 3.0 license

It is very common to see code directly copied from answers



site design / logo © 2018 Stack Exchange Inc; user contributions licensed under cc by-sa 3.0 with attribution required.
rev 2018.11.6.32085

How to fix :

- Remove code
- Rewrite code
- Reach out to Author on Stackoverflow and ask for different license
- Beware of ownership issues, do they have permission to relicense code in first place?

Compliance Issue: Cut&Pastes w/o license text

Developers will often cut and paste useful routines or files

In many cases the original Copyright and License Text is removed or lost

There may be comments such as “Stolen from http://” or “code from…”

How to fix:

- Identify the origin and the license
- If the license is unacceptable, remediate as usual
- Pay special attention to LGPL, cut&pasting may lead to static linking!
- Insert original copyright and license back into file
- Fulfill other license compliance actions (Notices, About box, Copyleft)

Compliance Issue: Undisclosed Webservices

It is becoming more common to depend on Webservices or Remote APIs

Common examples are time services, currency lookups, data feeds, etc..

These APIs often have Service Level Agreements or Terms of Use

Low use in development flies under the radar, but production use can be blocked

Netgear and the University of Wisconsin–Madison, embedded ntp server service in router ended up costing Netgear $375,000 in donations to UWM

Run wireshark and perform code scans

Best practice: Discover and track all Webservices and get clear SLA or self host

Compliance Issue: Multi-media (images, icons, sounds, clipart)

Multimedia items such as images, icons, sounds, fonts or clipart are often not treated as third party components though they contain licensing as well

Be careful of remotely hosted resources!

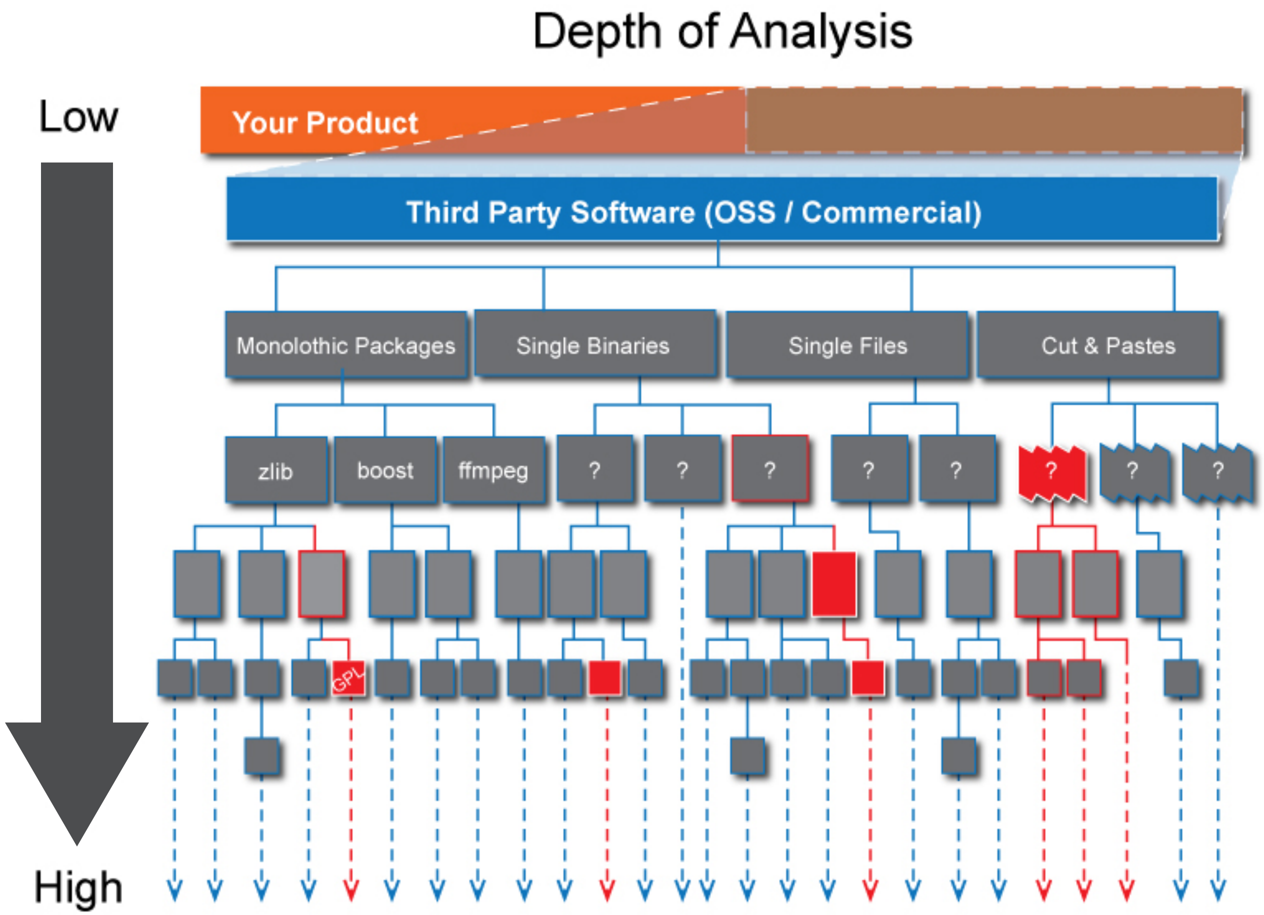
Watch for transformation of images (water mark removal, size, etc)!

How to fix:

- Identify license
- Remediate as usual

Compliance Issue: Subcomponent problems

It’s common to see “out of policy” licenses inside of “good” components



Compliance Issue: Subcomponent problems

The first step is to confirm that this licensed content is actually used

Build scripts, testing components, etc.. often have “out of policy” licenses but don’t link to or are not shipped with the top level component

If you find non-compliant actively used subcomponents you have a few options:

1) Fix it yourself and fork

2) Log a defect w/ the original component

3) Remove the full component and remediate

Compliance Issue: Lack of Attribution or Full Text

It is common to not receive the full OSS License or Copyright, especially when using a Repository Manager

Some components only mention high level licensing terms “This library is available under the terms of MIT license” or simply “MIT”

Best course of action is to reach out to the author and ask!

- Fedora tracks over 22 variants of the MIT license alone
- Https://fedoraproject.org/wiki/Licensing:MIT

Full license may be in the source bundle or code repository

Comply with Attribution requirements as best as possible

FLEXERA

Compliance Issue: Commercial Non-Compliance

Commercial software typically comes in 2 types

- Classic “commercially” licensed software for pay
- Free EULA click license w/ commercial terms

You may find these as both direct components or as subcomponents in other OSS projects

Often treated as a high priority by legal due to previous experience with similar issues

Treat in a similar fashion as “OSS Subcomponent problems”

Compliance Issue: Unknown licenses

Often seen in “old” components, especially in the Windows ecosystem

Also seen in scripts, small routines, gists and demos

The older something is, the harder it is to find out its license

Must weigh cost of detective work over “simple” remediation

The Wayback Machine is your friend! https://archive.org/web/

LinkedIn can be helpful for tracking down authors or companies

Compliance Issue: Patent issues

Patent licenses or royalties are hard to scan for

Often seen in Multimedia and Codec related components

Be alert any time audio or video is being transmitted or transcoded

ffmpeg, VideoLAN, H.264, etc..

How to fix:

- Pay patent royalty
- Remove and replace with Royalty free codec or component

Q&A

THANK YOU!

@ JLuszcz@Flexera.com

www.flexera.com

@JeffLuszcz