

TECH  
EXE  
TER \_

2019 CONFERENCE

TECH // HACK // DEVELOP

## Technical Due Diligence & Software Composition Analysis

Paul McAdam

Source Code Control Ltd

[paul.mcadam@sourcecodecontrol.co](mailto:paul.mcadam@sourcecodecontrol.co)

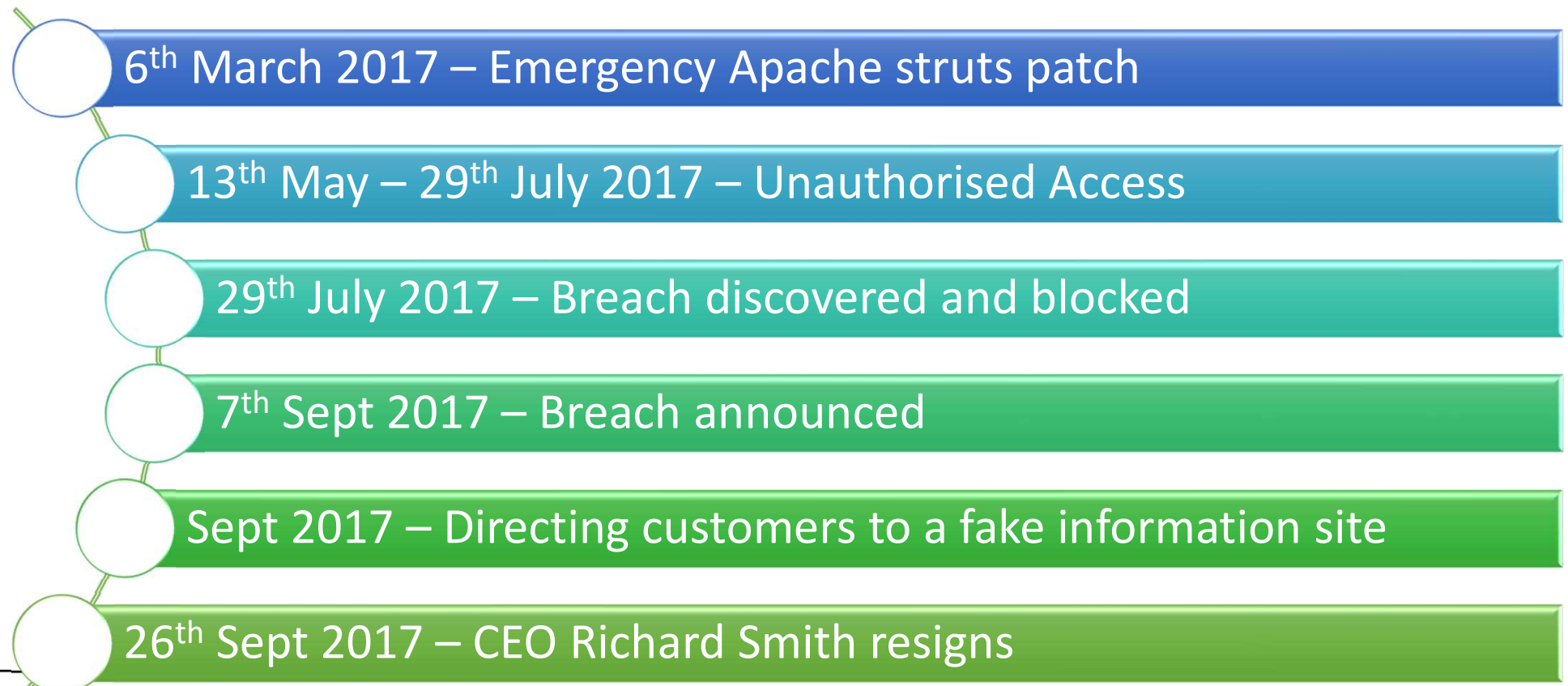
TECH  
EXE  
TER \_



**Source Code Control**  
*Open Source Risk Management Specialists*

©2019 Source Code Control Limited

# The Equifax Timeline



TECH  
EXE  
TER \_

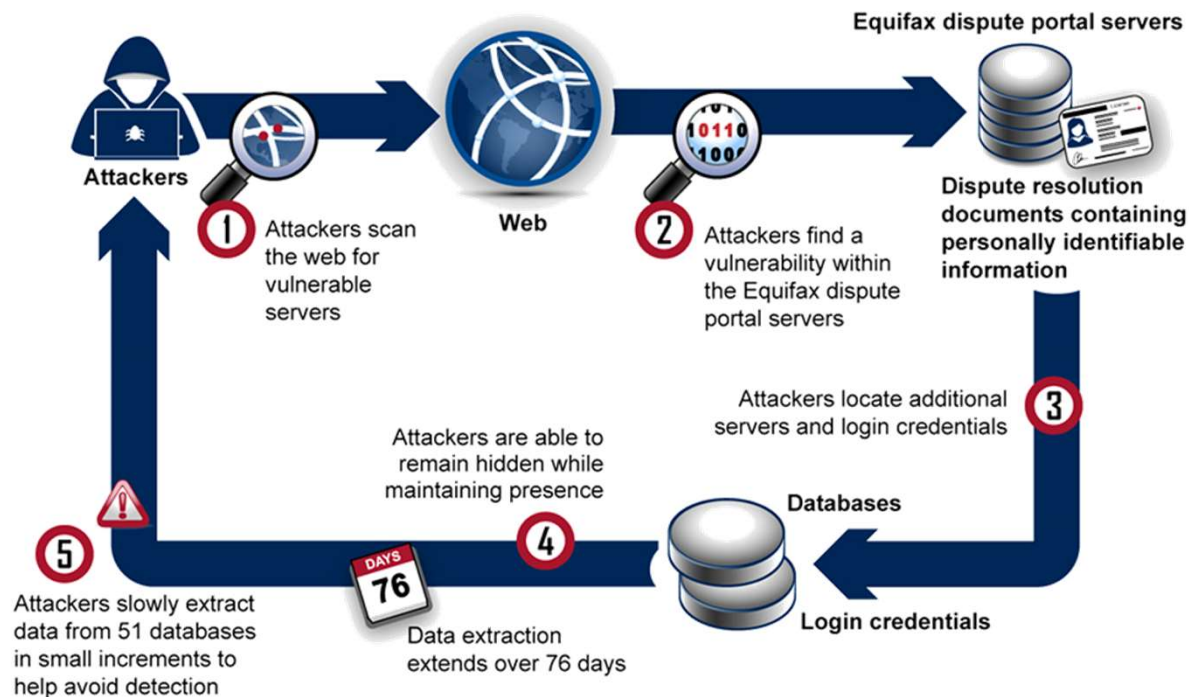


**Source Code Control**  
*Open Source Risk Management Specialists*

©2019 Source Code Control Limited

# How attackers exploited vulnerabilities

## How Attackers Exploited Vulnerabilities in the 2017 Breach, Based on Equifax Information



Source: GAO, based on information provided by Equifax. | GAO-18-559

**Problem 1: Ineffective Identification**

**Problem 2: Poor Detection**

**Problem 3: No Segmentation**

**Problem 4: Poor Data Governance**

**Bonus Problem: Apache Struts**

United States Government Accountability Office

TECH  
EXE  
TER \_



**Source Code Control**  
Open Source Risk Management Specialists

©2019 Source Code Control Limited

# Equifax Breach

EQUIHACKS

## The hackers who broke into Equifax exploited a flaw in open-source server software

```
1 /** The ContentTypeHandler Java class in Struts */
2 class ContentTypeHandler extends Interface {
3     ContentTypeHandler() {
4         this.hasQualifiedName("org.apache.struts2.rest.handler", "ContentTypeHandler")
5     }
6 }
```

```
8 /** The method `toObject` */
9 class ToObjectDeserializer extends Method {
10     ToObjectDeserializer() {
11         this.setSuperType(...)
12     }
13     .getASupertype*() instanceof ContentTypeHa
14     toObject(java.io.Reader, java.lang.Object)"
```

≡ Money

INVESTING • STOCKS

## Equifax's Massive Data Breach Has Cost the Company \$4 Billion So Far



- Apache Struts vulnerability
  - 2 vulnerabilities in 2017
  - March and September
  - 65% leading websites use Struts



Bloomberg

Markets

Tech

Pursuits

Politics

Opinion

Businessweek

## Equifax CEO Richard Smith Resigns After Uproar Over Massive Hack

By Jennifer Surane and Anders Melin

September 26, 2017, 3:02 PM GMT+1 Updated on September 26, 2017, 5:06 PM GMT+1

T  
E X E  
T E R \_



Source Code Control  
Open Source Risk Management Specialists

©2019 Source Code Control Limited

# 145.5m records!

*"As your company continues to issue incomplete, confusing and contradictory statements and hide information from Congress and the public, it is clear that five months after the breach was publicly announced, Equifax has yet to answer this simple question in full: what was the precise extent of the breach?"*

Senator Elizabeth Warren

TECH  
EXE  
TER \_



**Source Code Control**  
Open Source Risk Management Specialists


©2019 Source Code Control Limited

# Equifax – the scandal continues

## Oi, you. Equifax. Cough up half a million quid for fumbling 15 million Brits' personal info to hackers

UK watchdog demands max penalty after security snafu

By Chris Williams, Editor in Chief 20 Sep 2018 at 00:10

38  SHARE ▼



The UK's privacy watchdog wants to fine Equifax £500,000 (\$660,000) after hackers siphoned off 15 million Brits' info from the credit-score agency's databases.

TECH  
EXE  
TER \_



Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

[Home](#) [Your data matters](#) [For organisations](#) [Make a complaint](#) [Action we've taken](#)

[About the ICO](#) / [News and events](#) / [News and blogs](#) /

## Credit reference agency Equifax fined for security breach

Date **20 September 2018**

Type **News**

The Information Commissioner's Office (ICO) [issued Equifax Ltd with a £500,000 fine](#)  for failing to protect the personal information of up to 15 million UK citizens during a cyber attack in 2017.



**Source Code Control**  
Open Source Risk Management Specialists

©2019 Source Code Control Limited



# Equifax – and continues

## Former Equifax executive charged with insider trading after data breach

- Former chief information officer Jun Ying sold nearly \$1m in shares
- Ying allegedly learned of breach days before it was made public



## *Another Equifax Employee Faces Charge of Insider Trading After Big Breach*



The data breach exposed the sensitive details of more than 140 million consumers, including Social Security numbers, driver's license numbers and other information.

Kevin D. Liles for The New York Times

TECH  
EXE  
TER \_



**Source Code Control**  
Open Source Risk Management Specialists

©2019 Source Code Control Limited

# Impact



TECH  
EXE  
TER \_



**Source Code Control**  
Open Source Risk Management Specialists

©2019 Source Code Control Limited




# 2019 Open Source Risk and Security Analysis Report

- 96% of codebases audited in 2018 contained open source components
- 68% of codebases contained some form of license conflict
- 38% contained components with no identifiable license.
- 85% of codebases contained components > 4 years out-of-date or no dev in past 2 years.
- The average age of vulnerabilities was 6.6 years
- 43% of codebases scanned had vulnerabilities > 10 years old.
- 16,500 new vulnerabilities in 2018 and > 40% of codebases contained at least one high-risk vulnerability

# Rate my sandwich


Name: **Eat Breakfast before it' s'gone**



December  
31  
Saturday

Ingredients:

- [Bacon](#)
- [Egg](#)
- [Cheese](#)
- [Lettuce](#)

**McAdam's**  
  
**Best in Town!**

Search box

Calendar Control

Photo manager

Database

Cross reference  
V1.1; v2; v3 avail

	Updated	License	Licensing Risk?	Operational Risk?	Security Risk?
<b>Searchio v1.2</b>	12/12/2017	AGPL	Y		
<b>Datum v0.3</b>	01/02/2016	Apache-2.0	Y	Y	Maybe
<b>Photo-It v2.1</b>	12/03/2010	CC-BY-NC-1.0	Y	Maybe	
<b>MySQL v5.7.20</b>	16/10/2017	GPL-2.0+ (with caveats)	Y		
<b>Cross-Ref v1</b>	04/05/2014	WTFPL	Y	Y	Maybe

TECH  
EXE  
TER \_



**Source Code Control**  
Open Source Risk Management Specialists

©2019 Source Code Control Limited

# OPENCHAIN – an emerging standard

- OpenChain Project addresses the question of “how do I trust open source compliance in my supply chain”
- The OpenChain Project identifies and shares the core components of an open source software compliance program
- The core of the OpenChain Project is the **Specification**.  
<https://www.openchainproject.org>

More Trust=  
More Collaboration=  
More Efficiency



TECH  
EXE  
TER \_

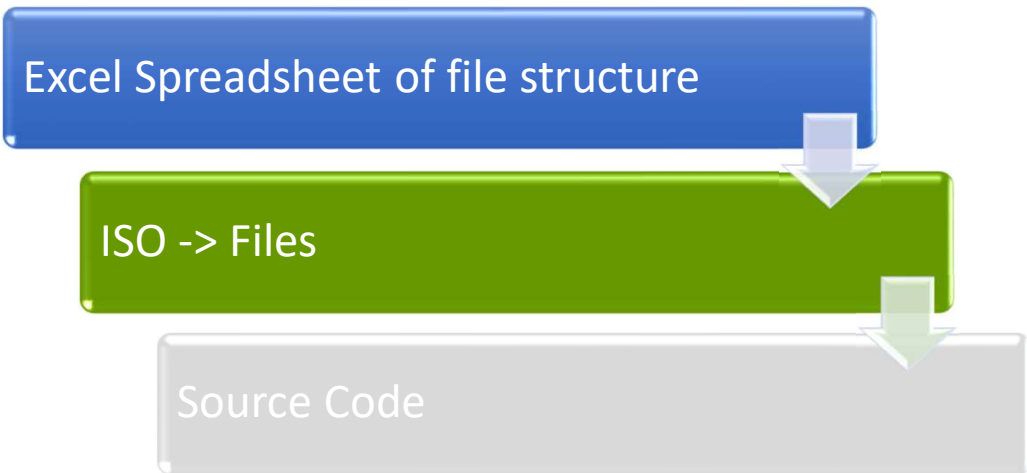


**Source Code Control**  
*Open Source Risk Management Specialists*

©2019 Source Code Control Limited

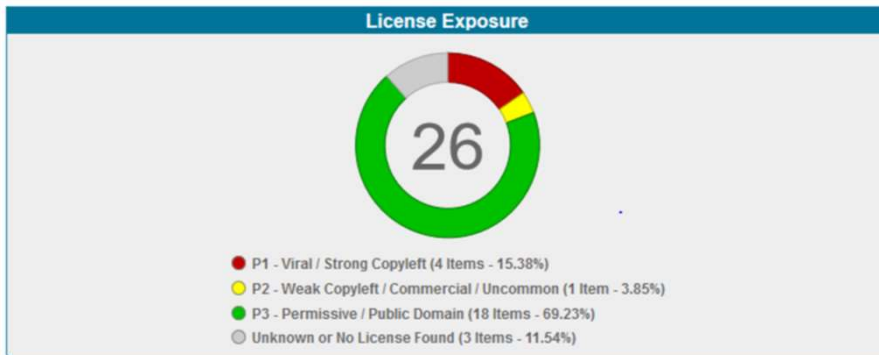
# Solution

- **Written in .NET**
- **Technical Availability:**
  - Hosted
  - On server
  - Standalone
  - Tablet and Phone interfaces



# Software Composition Analysis

- 5,602 files scanned
- 135,267 lines of code examined





# Package Components

Name	Component	License	Vulnerabilities			
jquery 1.3.2 (See Detection Notes)	jquery - 1.3.2	None Selected	3	0	3	0
zlib 1.2.1 (Zlib)	zlib - 1.2.1	zlib License	2	1	0	1
jQuery 1.10.2 (MIT)	jquery - 1.10.2	MIT License (also X11)	2	0	2	0
zlib 1 (zlib/libpng License)	zlib - 1	zlib/libpng License	1	1	0	0
zlib 1.0.4 (Zlib)	zlib - 1.0.4	zlib License	1	1	0	0
zlib 1.0.4 (zlib/libpng License)	zlib - 1.0.4	zlib/libpng License	1	1	0	0
zlib 1.1.3 (Zlib)	zlib - 1.1.3	zlib License	1	1	0	0
zlib 1.1.4 (Zlib)	zlib - 1.1.4	zlib License	1	1	0	0
jQuery - NuGet 2.1.3 (MIT)	jquery - 2.1.3	MIT License (also X11)	1	0	1	0
jquery 2.2.4 (MIT)	jquery - 2.2.4	MIT License (also X11)	1	0	1	0
libjpeg 6b (IJG)	libjpeg - 6b	Independent JPEG Group License	1	0	1	0
App Browsers (GPL-2.0)	app - browsers	GNU General Public License v2.0	0	0	0	0
App Code (GPL-2.0)	app - code	GNU General Public License v2.0	0	0	0	0
App global.asax (GPL-2.0)	app - global.asax	GNU General Public License v2.0	0	0	0	0
App Licenses (GPL-2.0)	app - licenses	GNU General Public License v2.0	0	0	0	0
Bootstrap 3 Typeahead 3.1.1 (Unknown License)	bootstrap-3-typeahead - 3.1.1	None Selected	0	0	0	0
Entity Framework 6.1.3 (Microsoft .NET Library EULA)	erisidcord-spout-textile - 1.4.3	Microsoft Visual Studio 2005 and .NET Framework 2.0 Samples EULA	0	0	0	0
jQuery - NuGet (MIT)	None Found	MIT License (also X11)	0	0	0	0
jquery 1.12.0 (See Detection Notes)	jquery - 1.12.0	None Selected	0	0	0	0
jquery 2.2.0 (MIT)	jquery - 2.2.0	MIT License (also X11)	0	0	0	0
Json.NET (MIT License)	None Found	MIT License (also X11)	0	0	0	0
Microsoft Exchange WebServices 2.2.0 (MIT License)	microsoft.exchange.webservices - 2.2.0	MIT-Style License	0	0	0	0
MiniProfiler 2.0.2 (Apache 2.0)	miniprofiler - 2.0.2	Apache License 2.0	0	0	0	0
Modernizr 2.8.3 (MIT)	modernizr - 2.8.3	MIT-Style License	0	0	0	0
Respond JS 1.4.1 (MIT)	respond - 1.4.1	MIT-Style License	0	0	0	0
Sizzle (MIT)	None Found	MIT License (also X11)	0	0	0	0

Remember: this is a .Net app – not intentionally Open Source

TECH  
EXE  
TER \_



**Source Code Control**  
Open Source Risk Management Specialists

©2019 Source Code Control Limited

# Open Source License Requirements

- **Copyright notice** - an identifier placed on copies of the work to inform the world of copyright ownership. Example: *Copyright © 2016 A. Person*
- **Licence notice** - a notice that specifies and acknowledges the licence terms and conditions of the open source software included in the product.
- **Attribution notice** - a notice included in the product release that acknowledges the identity of the original authors and/or sponsors of the open source software included in the product.
- **Modification notice** – a notice that you have made modifications to the source code of a file, such as adding your copyright notice to the top of the file.

The MIT License (MIT)

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including

with  
mer  
copi  
whc  
the

The zlib/libpng License Copyright (c)

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

**The notice portion** Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such and must not be misrepresented as being the original software.

**3. This notice may not be removed or altered from any source distribution.**

TECH  
EXE  
TER \_



**Source Code Control**  
Open Source Risk Management Specialists

©2019 Source Code Control Limited

# GPL Licenses

- 4 GPL Licences discovered
- **Reciprocity – MUST** license the whole work under the GPLv2.0 licence. This would conflict with the proprietary licence or End User Licence Agreement of Application.
- **Source code availability – MUST** offer the source code to users of the software. This requires supplying the EXACT version of the source code.

## TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) **You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.**

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) **Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code,** to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or..

# 15 security vulnerabilities

Component	Vuln	Risk
ZLIB 1.2.1	CVE-2005-2096	High
	CVE-2004-0797	Low
ZLIB 1.1.4	CVE-2003-0107	High
ZLIB 1.1.3	CVE-2003-0107	High
ZLIB 1.0.4 (x2)	CVE-2002-0059	High
ZLIB 1	CVE-2002-0059	High
LIBJPEG 6B	CVE-2013-6629	Medium
JQUERY 2.2.4	CVE-2011-9251	Medium
JQUERY 1.3.2	CVE-2011-4969	Medium
	CVE-2012-6708	Medium
	CVE-2015-9251	Medium
JQUERY 1.10.2	CVE-2012-6708	Medium
	CVE-2015-9251	Medium
JQUERY 2.1.3	CVE-2015-9251	Medium

Issues dating  
back to 2002

Multiple versions  
of the same  
components

No patching  
strategy

TECH  
EXE  
TER \_



**Source Code Control**  
Open Source Risk Management Specialists

©2019 Source Code Control Limited

# Our Conclusions

- No code maintenance / patching despite obvious re-use of historic code
- No open source software policy
- No ability to identify open source components
- No understanding of licensing and IP obligations of open source licensing
- No managerial responsibility for licence compliance
- No supply of required documentation and artifacts required to comply with the licences of components used by developers
- No structure to manage security vulnerabilities in their supply chain

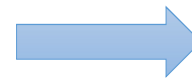


# Recent example

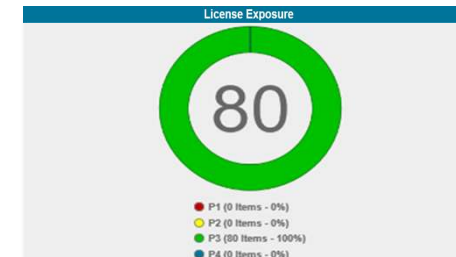
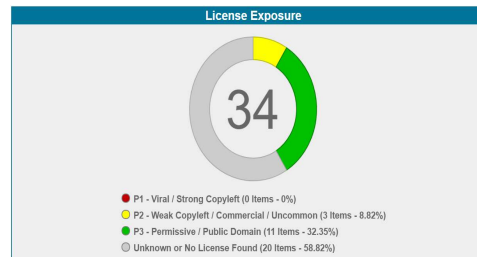
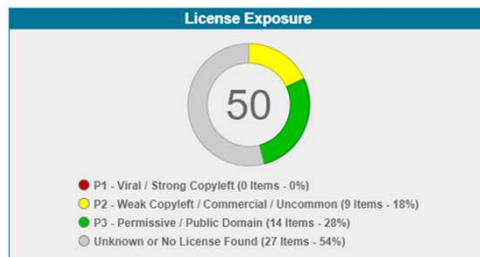
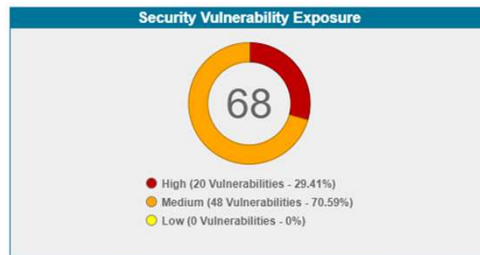
1,317 Files  
139,570 lines of code  
1 AGPL item



1,027 Files  
215,751 lines of code  
No copyleft



1,400 Files  
112,297 lines of code  
No copyleft



*"I would like to say a big thank you for moving this project along with pace. Your approach of keeping the client abreast of issues as they arise and including the chance to remediate prior to final testing was a refreshing change"*

Owner, Risk Management Consultancy

TECH  
EXE  
TER \_



**Source Code Control**  
Open Source Risk Management Specialists

©2019 Source Code Control Limited