Global Forum
Shaping the future 2015

A Call For A Cybersecurity Social Contract

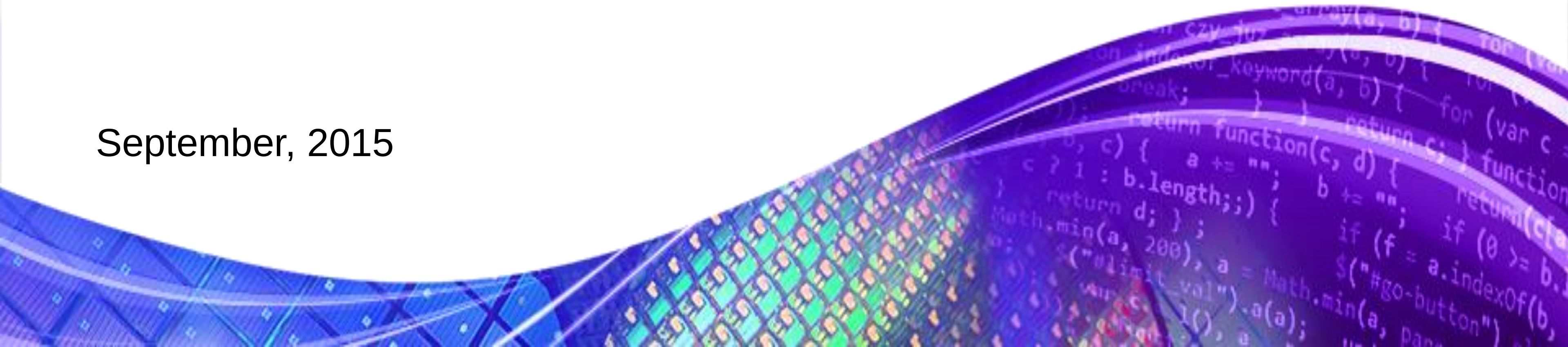
A request to software companies to act more responsibly

SYNOPSYS®
Silicon to Software™

Presented By:

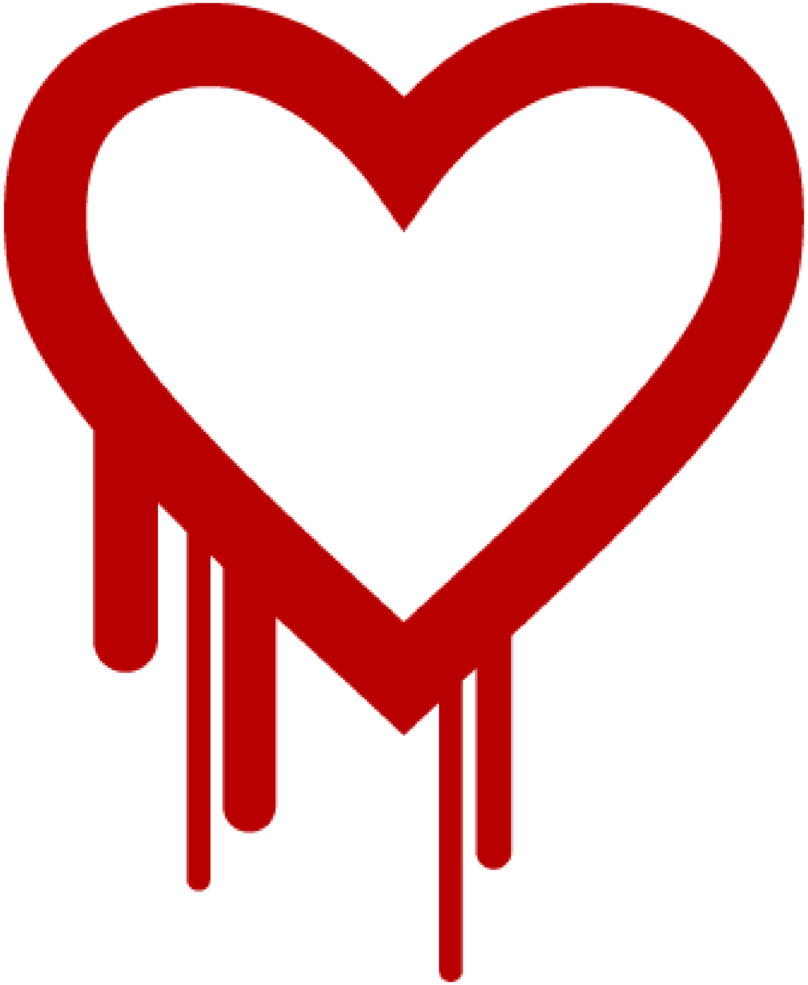
Mike Ahmadi,
Global Director Critical Systems Security,
Synopsys Software Integrity Group

September, 2015



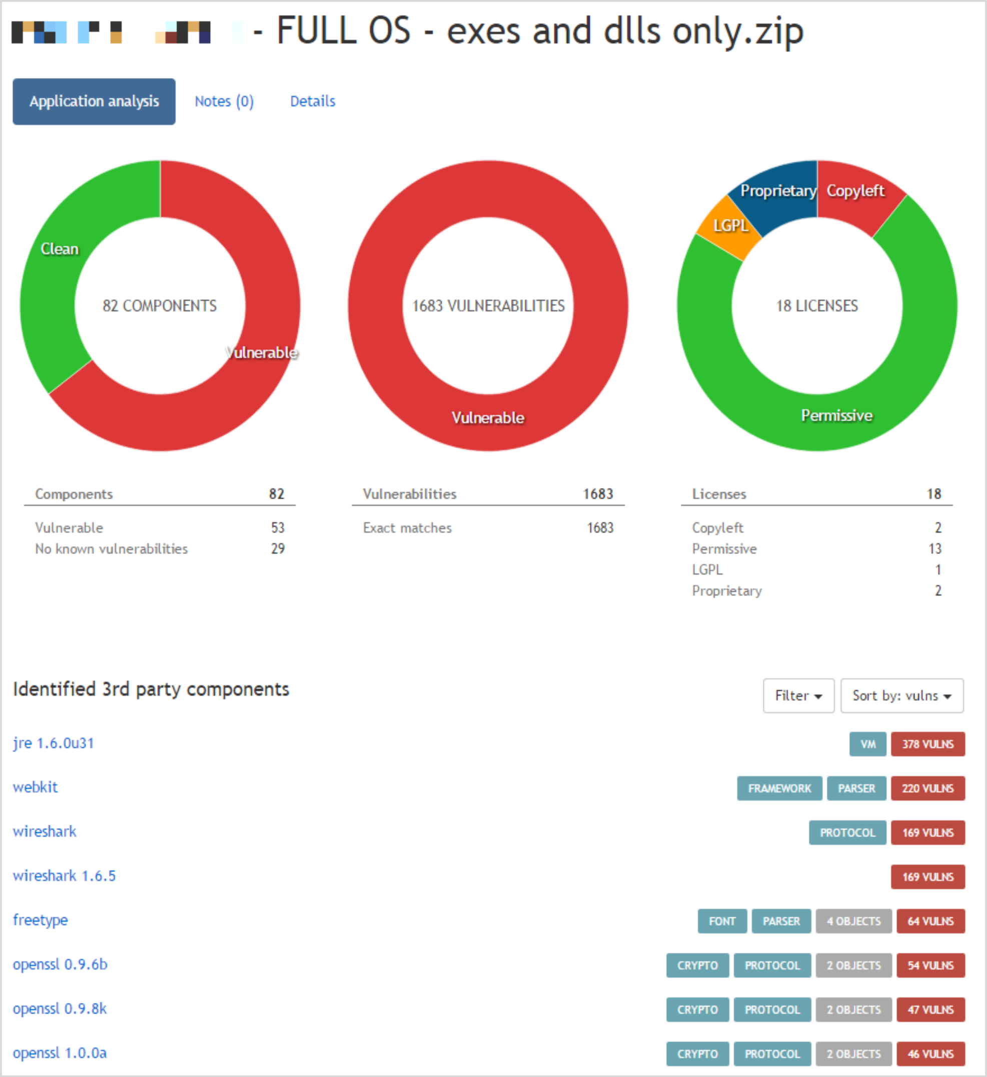
Zero Days Are Very Interesting

- A 0-Day is a previously unknown bug
- Particularly challenging because they are a big unknown
- They get a lot of attention
- They are like needles in a haystack



Unknown Vulnerabilities Are **Bad**… Known Vulnerabilities Are A **HUGE** Problem

- Hospital central monitoring system with **1683 known vulnerabilities**
- 378 of the vulnerabilities are in one (Java) runtime environment, meaning **just updating the version will fix 378 vulnerabilities.**
- This **system** is **widely used** throughout hospitals…including government hospitals



[redacted] - FULL OS - exes and dlls only.zip

Components	82
Vulnerable	53
No known vulnerabilities	29

Vulnerabilities	1683
Exact matches	1683

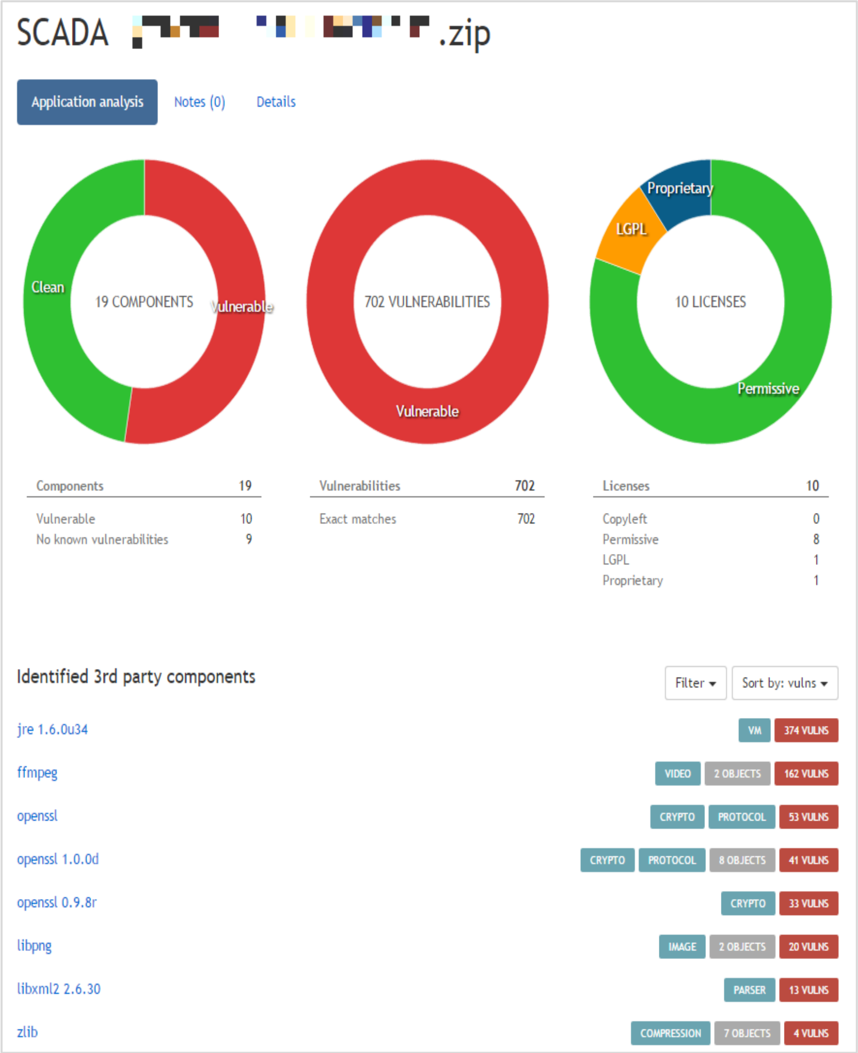
Licenses	18
Copyleft	2
Permissive	13
LGPL	1
Proprietary	2

Identified 3rd party components

jre 1.6.0u31	VM 378 VULNS
webkit	FRAMEWORK PARSER 220 VULNS
wireshark	PROTOCOL 169 VULNS
wireshark 1.6.5	169 VULNS
freetype	FONT PARSER 4 OBJECTS 64 VULNS
openssl 0.9.6b	CRYPTO PROTOCOL 2 OBJECTS 54 VULNS
openssl 0.9.8k	CRYPTO PROTOCOL 2 OBJECTS 47 VULNS
openssl 1.0.0a	CRYPTO PROTOCOL 2 OBJECTS 46 VULNS

Let’s look at an industrial control system

- SCADA system with over **20,000 licenses worldwide**
- **Customer reference list on website (including government customers)**
- **702 exact match vulnerabilities** in 10 components.
- **374 vulnerabilities in 1 java runtime**
- **Over 150** NIST CVSS **critical in one component**



SCADA [redacted] .zip

Application analysis Notes (0) Details

Components	19
Vulnerable	10
No known vulnerabilities	9

Vulnerabilities	702
Exact matches	702

Licenses	10
Copyleft	0
Permissive	8
LGPL	1
Proprietary	1

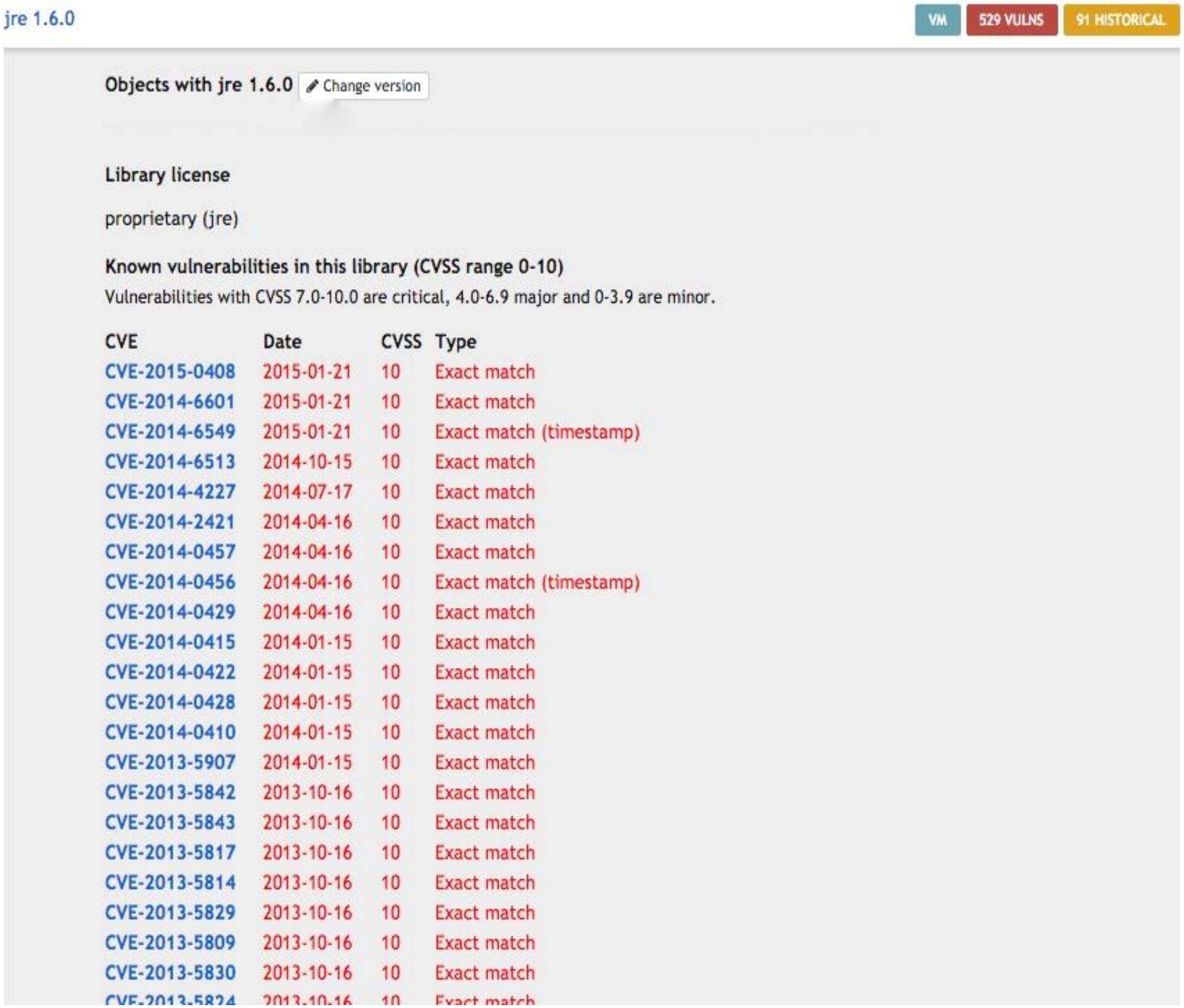
Identified 3rd party components

Filter ▾ Sort by: vulns ▾

jre 1.6.0u34			VM	374 VULNS
ffmpeg		VIDEO	2 OBJECTS	162 VULNS
openssl		CRYPTO	PROTOCOL	53 VULNS
openssl 1.0.0d	CRYPTO	PROTOCOL	8 OBJECTS	41 VULNS
openssl 0.9.8r			CRYPTO	33 VULNS
libpng		IMAGE	2 OBJECTS	20 VULNS
libxml2 2.6.30			PARSER	13 VULNS
zlib		COMPRESSION	7 OBJECTS	4 VULNS

Serious Nature of Specific Vulnerabilities

- Over **150 vulnerabilities** in Java scored **CRITICAL**
- Critical commonly means **remotely executable with no authentication**
- This means that there are potentially at least **150 fairly trivial ways to exploit** the system



Objects with jre 1.6.0

Library license

proprietary (jre)

Known vulnerabilities in this library (CVSS range 0-10)

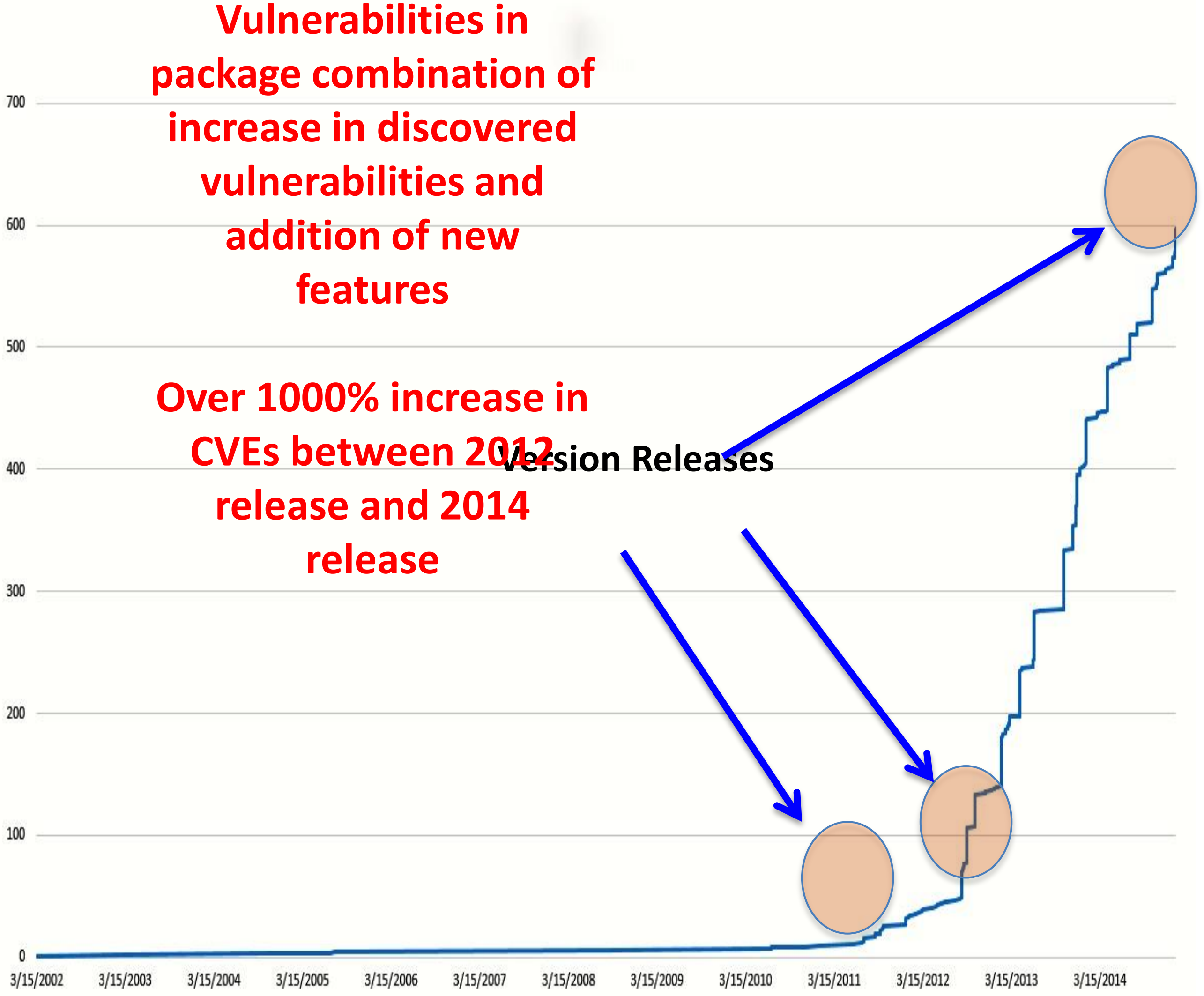
Vulnerabilities with CVSS 7.0-10.0 are critical, 4.0-6.9 major and 0-3.9 are minor.

CVE	Date	CVSS	Type
CVE-2015-0408	2015-01-21	10	Exact match
CVE-2014-6601	2015-01-21	10	Exact match
CVE-2014-6549	2015-01-21	10	Exact match (timestamp)
CVE-2014-6513	2014-10-15	10	Exact match
CVE-2014-4227	2014-07-17	10	Exact match
CVE-2014-2421	2014-04-16	10	Exact match
CVE-2014-0457	2014-04-16	10	Exact match
CVE-2014-0456	2014-04-16	10	Exact match (timestamp)
CVE-2014-0429	2014-04-16	10	Exact match
CVE-2014-0415	2014-01-15	10	Exact match
CVE-2014-0422	2014-01-15	10	Exact match
CVE-2014-0428	2014-01-15	10	Exact match
CVE-2014-0410	2014-01-15	10	Exact match
CVE-2013-5907	2014-01-15	10	Exact match
CVE-2013-5842	2013-10-16	10	Exact match
CVE-2013-5843	2013-10-16	10	Exact match
CVE-2013-5817	2013-10-16	10	Exact match
CVE-2013-5814	2013-10-16	10	Exact match
CVE-2013-5829	2013-10-16	10	Exact match
CVE-2013-5809	2013-10-16	10	Exact match
CVE-2013-5830	2013-10-16	10	Exact match
CVE-2013-5824	2013-10-16	10	Exact match

Unique Vulnerabilities Graph Over Time

- **Huge increase** in number of vulnerabilities entering **NIST CVE database** in the last 3 years

- **Massive spike since 2013** for common software components (such as Java, OpenSSL)

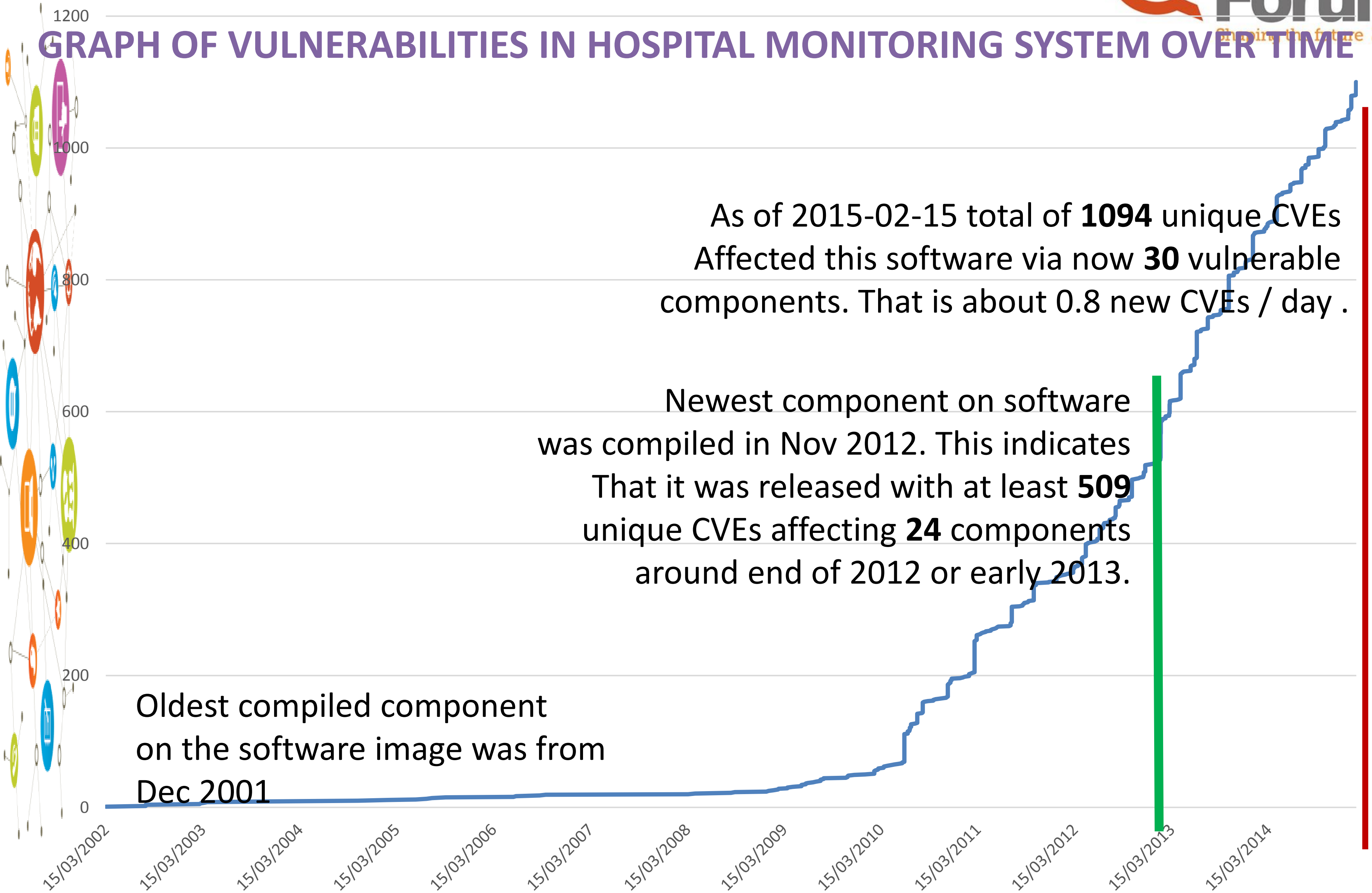


Vulnerabilities in package combination of increase in discovered vulnerabilities and addition of new features

Over 1000% increase in CVEs between 2012 release and 2014 release

Version Releases

GRAPH OF VULNERABILITIES IN HOSPITAL MONITORING SYSTEM OVER TIME

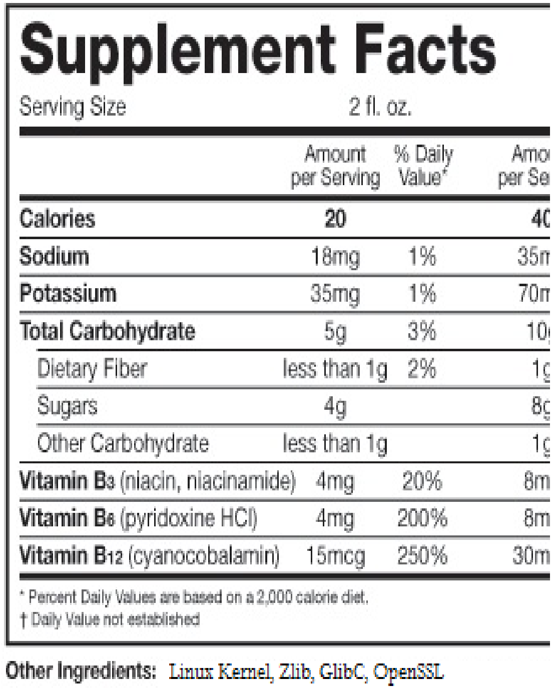


As of 2015-02-15 total of **1094** unique CVEs Affected this software via now **30** vulnerable components. That is about 0.8 new CVEs / day .

Newest component on software was compiled in Nov 2012. This indicates That it was released with at least **509** unique CVEs affecting **24** components around end of 2012 or early 2013.

Oldest compiled component on the software image was from Dec 2001

Why not?



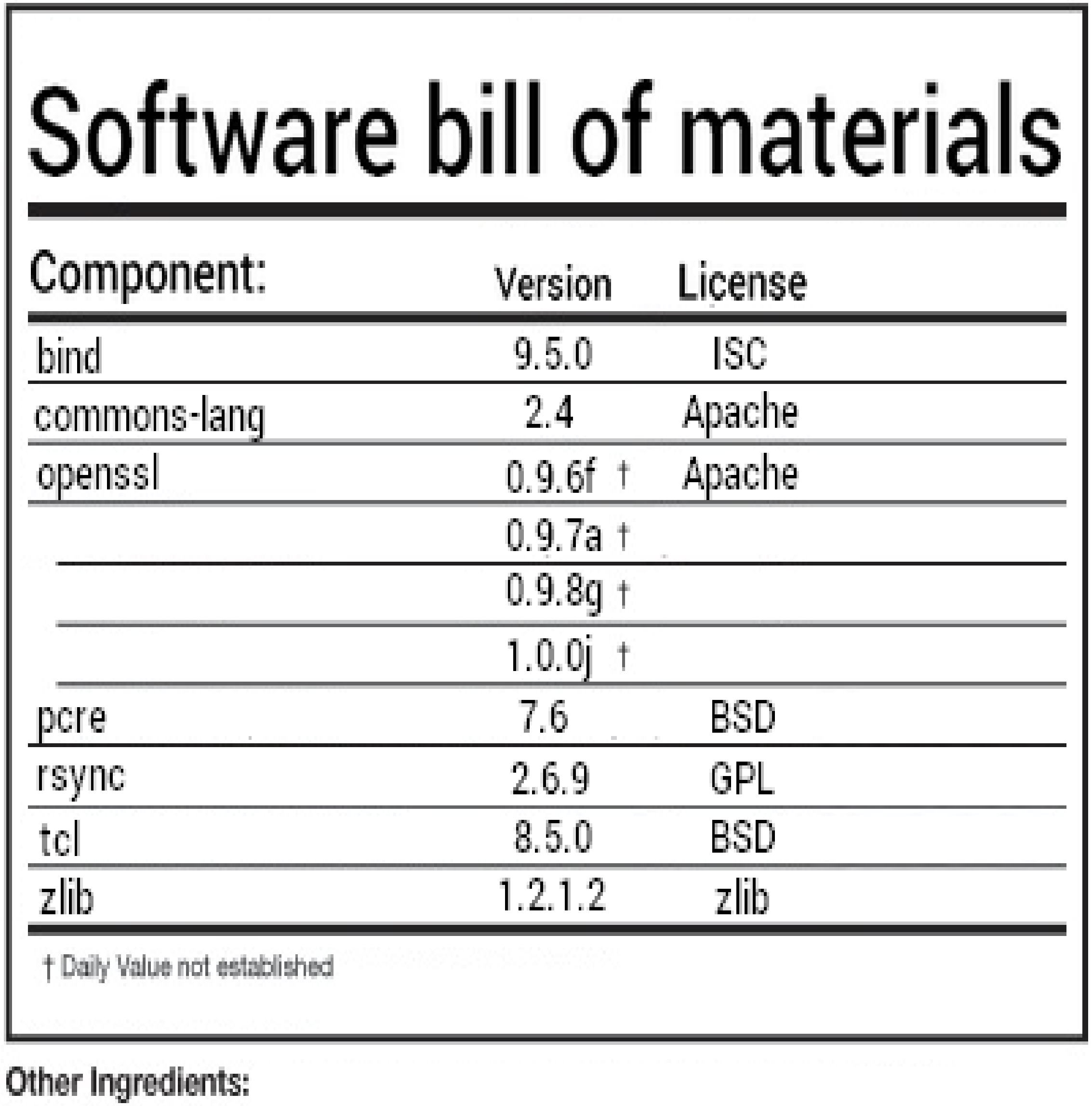
Supplement Facts

Serving Size 2 fl. oz.

	Amount per Serving	% Daily Value*	Amo per Se
Calories	**20**		**40**
Sodium	18mg	1%	35m
Potassium	35mg	1%	70m
Total Carbohydrate	5g	3%	10
Dietary Fiber	less than 1g	2%	1g
Sugars	4g		8g
Other Carbohydrate	less than 1g		1g
Vitamin B3 (niacin, niacinamide)	4mg	20%	8m
Vitamin B6 (pyridoxine HCl)	4mg	200%	8m
Vitamin B12 (cyanocobalamin)	15mcg	250%	30m

* Percent Daily Values are based on a 2,000 calorie diet.
† Daily Value not established

Other Ingredients: Linux Kernel, Zlib, GlibC, OpenSSL



Software bill of materials

Component:	Version	License
bind	9.5.0	ISC
commons-lang	2.4	Apache
openssl	0.9.6f †	Apache
	0.9.7a †	
	0.9.8g †	
	1.0.0j †	
pcre	7.6	BSD
rsync	2.6.9	GPL
tcl	8.5.0	BSD
zlib	1.2.1.2	zlib

† Daily Value not established

Other Ingredients:

Opposition Arguments

- **We already do this:** The data indicates that if this is already being done no action is being taken to resolve the issue. More likely it is not being done…or being done quite poorly, and leaving us all at risk.
- **Sharing a Bill of Materials means giving up proprietary information:** FDA already requires an ingredient list. Coca Cola can supply an ingredient list without sharing trade secrets.
- **I cannot control my supply chain:** You already do in selection of products based on feature requirements.
- **This requires too much work:** Tools are completely automated and easy to use.

Ultimately the software industry can expempt themselves from liabilities due to ANY software failures because the law lets them do so. Software is the only industry that can get away with this!

What They Are Really Saying

- We don’t want to know about it.
- We don’t want to tell anyone about it.
- We don’t want to fix it.
- …but we still want you to buy it.

PROJECT MANAGER
EXECUTIVE
VENDOR

I don’t think that is reasonable !

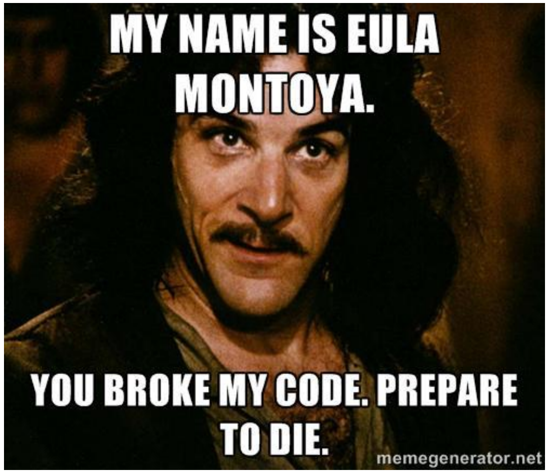
We Are The Software Company. Trust Us…Or Else!

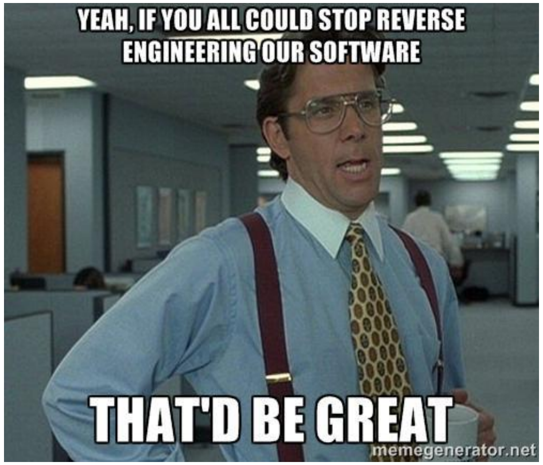
INCONET-GCC 2

شبكة التعاون الدولية للعلوم التكنولوجيا (الاتحاد الأوروبي - دول مجلس التعاون الخليجي)

EU-GCC Science & Technology International Cooperation Network

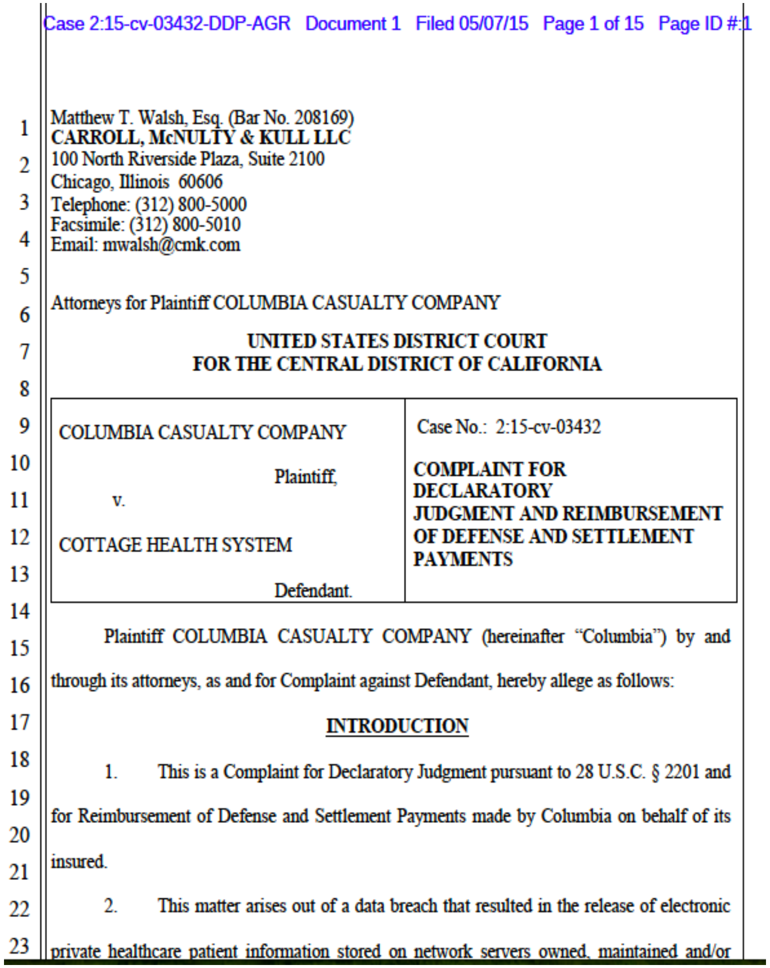
- CSO of a large software company recently posted a blog admonishing organizations that analyze their code…or hire others to do so.
- This did not bode well with the security world.
- Fortunately, the company took down the blog post and stated that the sentiments expressed in the blog did not represent the organization's sentiment.




YEAH, IF YOU ALL COULD STOP REVERSE ENGINEERING OUR SOFTWARE
THAT'D BE GREAT
memegenerator.net

The Insurance Industry Pushes Back

- Cottage Health System gets breached forced to pay class action settlement of $4.125 million ($81 per record)
- Insurer files suit in court for a Declaratory Judgment against Columbia for Cottage's "**Failure to Follow Minimum Required Practices.**"



Case 2:15-cv-03432-DDP-AGR Document 1 Filed 05/07/15 Page 1 of 15 Page ID #:1

Matthew T. Walsh, Esq. (Bar No. 208169)
CARROLL, McNULTY & KULL LLC
100 North Riverside Plaza, Suite 2100
Chicago, Illinois 60606
Telephone: (312) 800-5000
Facsimile: (312) 800-5010
Email: mwalsh@cmk.com

Attorneys for Plaintiff COLUMBIA CASUALTY COMPANY

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

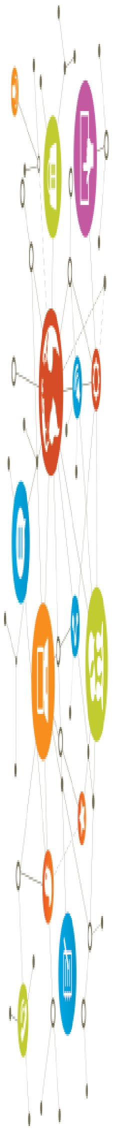
COLUMBIA CASUALTY COMPANY Plaintiff, v. COTTAGE HEALTH SYSTEM Defendant.	Case No.: 2:15-cv-03432 **COMPLAINT FOR DECLARATORY JUDGMENT AND REIMBURSEMENT OF DEFENSE AND SETTLEMENT PAYMENTS**

Plaintiff COLUMBIA CASUALTY COMPANY (hereinafter "Columbia") by and through its attorneys, as and for Complaint against Defendant, hereby allege as follows:

INTRODUCTION

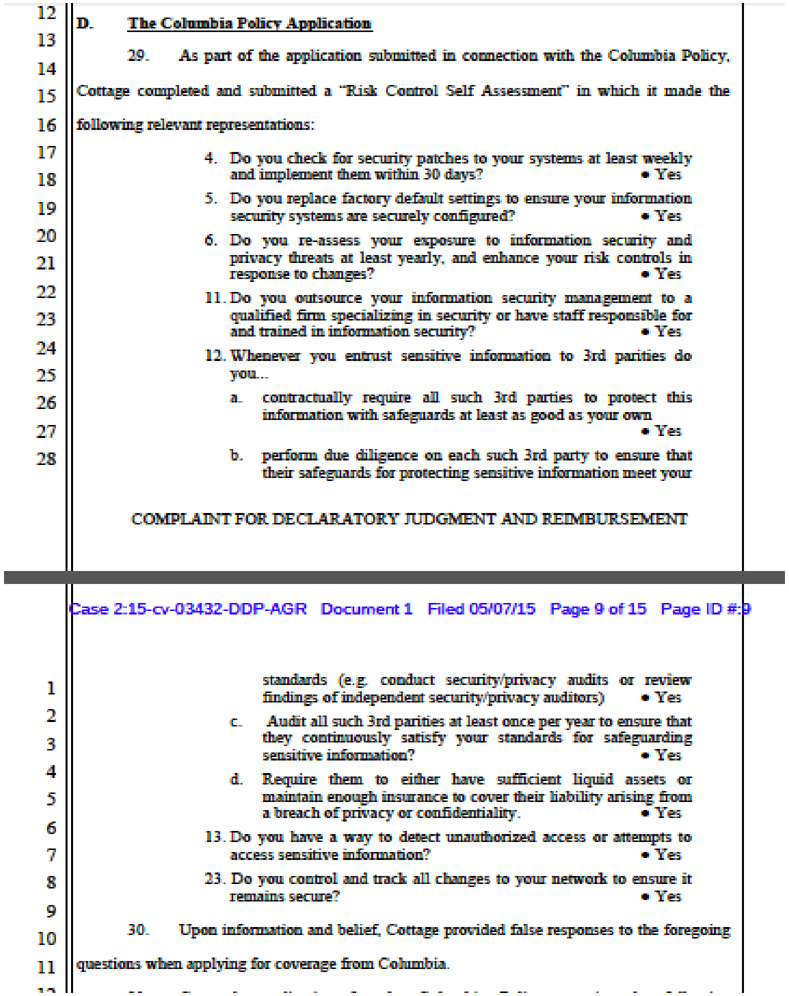
1. This is a Complaint for Declaratory Judgment pursuant to 28 U.S.C. § 2201 and for Reimbursement of Defense and Settlement Payments made by Columbia on behalf of its insured.

2. This matter arises out of a data breach that resulted in the release of electronic private healthcare patient information stored on network servers owned, maintained and/or



Some Minimum Required Practices In Detail

- Check for security patches and apply within 30 days
- Replace factory default settings
- Re-assess risk yearly and apply changes
- Require 3rd parties to protect information with safeguards at least as good as your own
- **PERFORM DUE DILLIGENCE ON 3RD PARTIES TO ENSURE THAT THEIR SAFEGUARDS ARE AS GOOD AS YOUR OWN**
- **AUDIT 3RD PARTIES TO ENSURE THEY CONTINUOSLY SATISFY YOUR STANDARDS FOR SAFEGUARDING SENSITIVE INFORMATION**



D. **The Columbia Policy Application**

29. As part of the application submitted in connection with the Columbia Policy, Cottage completed and submitted a "Risk Control Self Assessment" in which it made the following relevant representations:

4. Do you check for security patches to your systems at least weekly and implement them within 30 days? • Yes
5. Do you replace factory default settings to ensure your information security systems are securely configured? • Yes
6. Do you re-assess your exposure to information security and privacy threats at least yearly, and enhance your risk controls in response to changes? • Yes
11. Do you outsource your information security management to a qualified firm specializing in security or have staff responsible for and trained in information security? • Yes
12. Whenever you entrust sensitive information to 3rd parities do you...
    a. contractually require all such 3rd parties to protect this information with safeguards at least as good as your own • Yes
    b. perform due diligence on each such 3rd party to ensure that their safeguards for protecting sensitive information meet your

COMPLAINT FOR DECLARATORY JUDGMENT AND REIMBURSEMENT

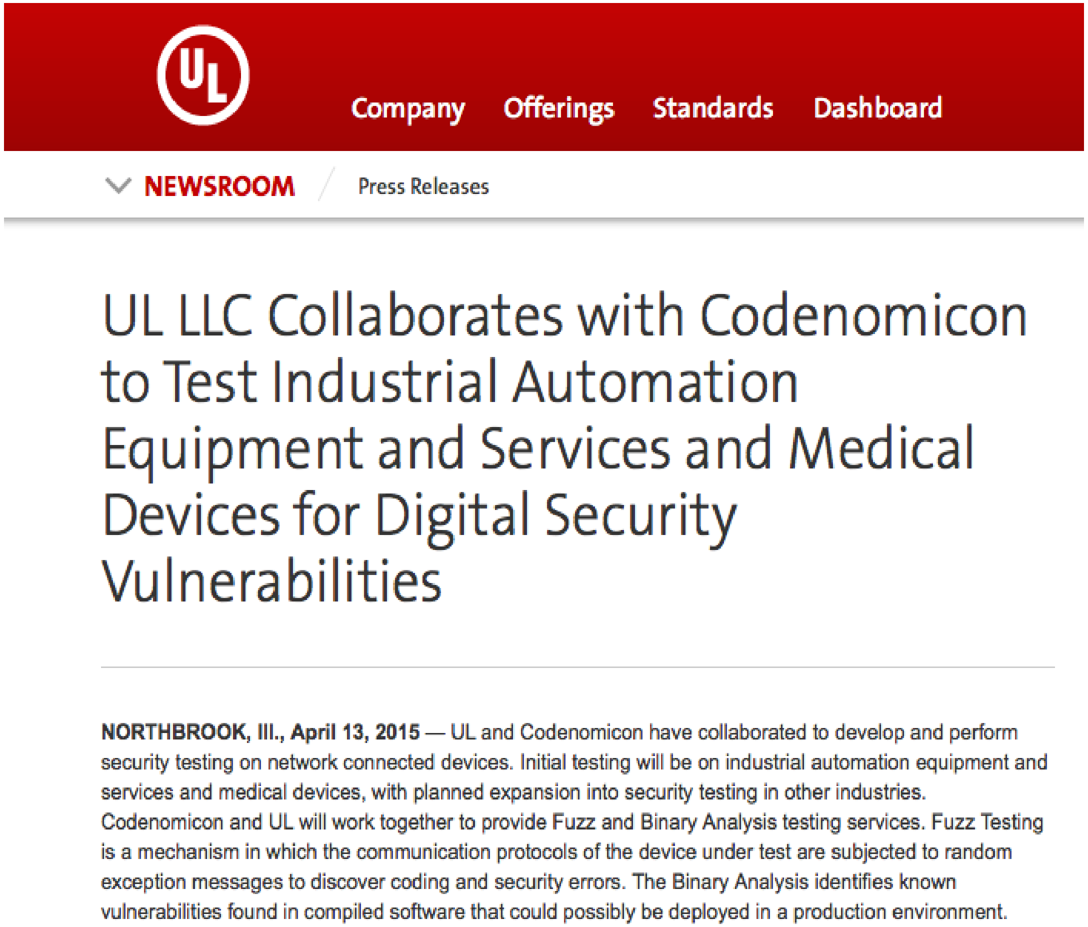
Case 2:15-cv-03432-DDP-AGR Document 1 Filed 05/07/15 Page 9 of 15 Page ID #:9

standards (e.g. conduct security/privacy audits or review findings of independent security/privacy auditors) • Yes

    c. Audit all such 3rd parities at least once per year to ensure that they continuously satisfy your standards for safeguarding sensitive information? • Yes
    d. Require them to either have sufficient liquid assets or maintain enough insurance to cover their liability arising from a breach of privacy or confidentiality. • Yes
13. Do you have a way to detect unauthorized access or attempts to access sensitive information? • Yes
23. Do you control and track all changes to your network to ensure it remains secure? • Yes

30. Upon information and belief, Cottage provided false responses to the foregoing questions when applying for coverage from Columbia.

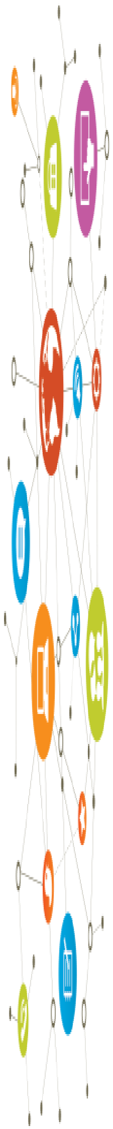
Building A Cybersecurity Certification Lab



UL LLC Collaborates with Codenomicon to Test Industrial Automation Equipment and Services and Medical Devices for Digital Security Vulnerabilities

NORTHBROOK, Ill., April 13, 2015 — UL and Codenomicon have collaborated to develop and perform security testing on network connected devices. Initial testing will be on industrial automation equipment and services and medical devices, with planned expansion into security testing in other industries. Codenomicon and UL will work together to provide Fuzz and Binary Analysis testing services. Fuzz Testing is a mechanism in which the communication protocols of the device under test are subjected to random exception messages to discover coding and security errors. The Binary Analysis identifies known vulnerabilities found in compiled software that could possibly be deployed in a production environment.

- **Aligned with international standards (62443)**
- **Creating program due to demand**
- **Creating program due to need**
- **Active lobbying to promote message**



Thank You!

Mike Ahmadi