Software Bill of Materials (SBOM) Primer

Joshua Corman
@joshcorman

NTIA Supply Chain Transparency
07/19/2018

Where Bits & Bytes meet Flesh & Blood

I am The Cavalry

HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

June 2017

REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY

INGREDIENTS: SUGAR, VEGETABLE OIL (PARTIALLY HYDROGENATED PALM KERNEL AND/OR COTTONSEED OIL, SOYBEAN AND PALM OIL), ENRICHED FLOUR (WHEAT FLOUR, NIACIN, REDUCED IRON, THIAMIN MONONITRATE [VITAMIN B1], RIBOFLAVIN [VITAMIN B2], FOLIC ACID), CORN SYRUP, COCONUT, SWEETENED CONDENSED MILK (CONDENSED MILK, SUGAR), CONTAINS TWO PERCENT OR LESS OF SORBITOL, COCOA, GLYCERIN, INVERT SUGAR, COCOA PROCESSED WITH ALKALI, CORNSTARCH, SALT, CARAMELIZED SUGAR, DEXTROSE, SOY LECITHIN, NATURAL AND ARTIFICIAL FLAVORS, CARRAGEENAN, LEAVENING (BAKING SODA, MONOCALCIUM PHOSPHATE).

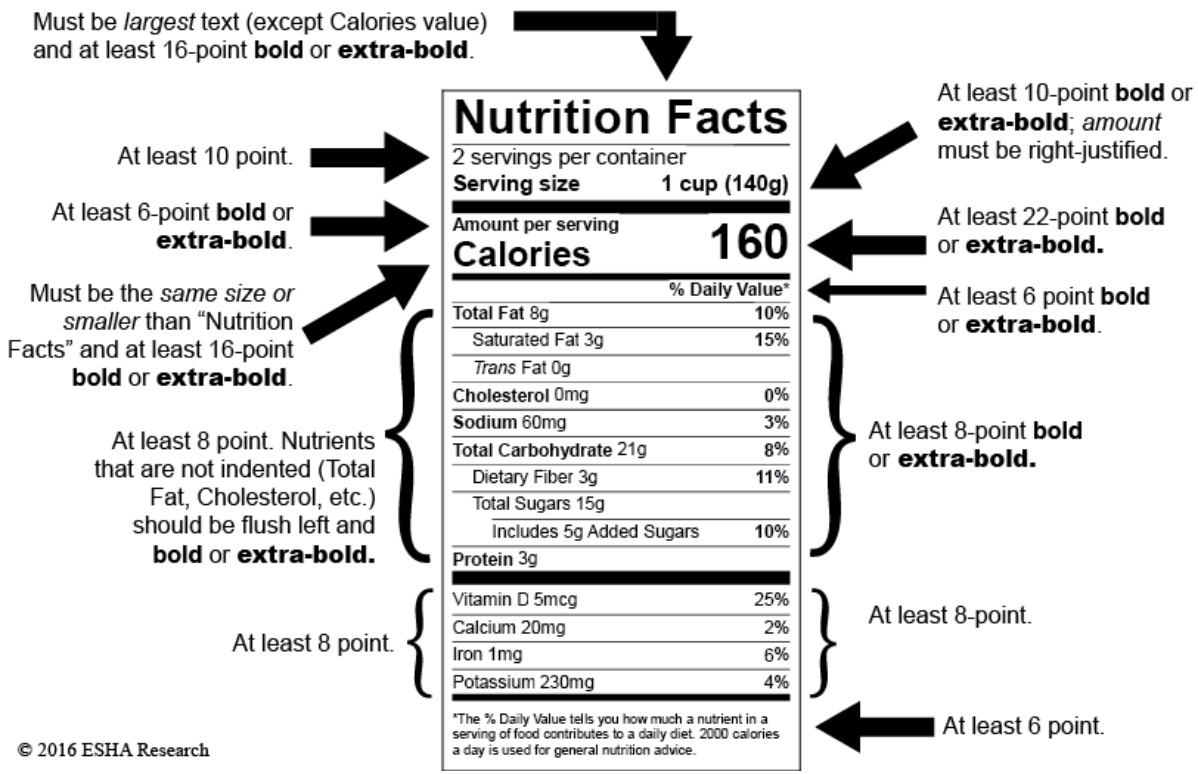
Allergen Information:

CONTAINS WHEAT, COCONUT, MILK, AND SOY INGREDIENTS.

INGREDIENTS: SUGAR, VEGETABLE OIL (PARTIALLY HYDROGENATED PALM KERNEL AND/OR COTTONSEED OIL, SOYBEAN AND PALM OIL), ENRICHED FLOUR (WHEAT FLOUR, NIACIN, REDUCED IRON, THIAMIN MONONITRATE [VITAMIN B1], RIBOFLAVIN [VITAMIN B2], FOLIC ACID), CORN SYRUP, COCONUT, SWEETENED CONDENSED MILK (CONDENSED MILK, SUGAR), CONTAINS TWO PERCENT OR LESS OF SORBITOL, COCOA, GLYCERIN, INVERT SUGAR, COCOA PROCESSED WITH ALKALI, CORNSTARCH, SALT, CARAMELIZED SUGAR, DEXTROSE, SOY LECITHIN, NATURAL AND ARTIFICIAL FLAVORS, CARRAGEENAN, LEAVENING (BAKING SODA, MONOCALCIUM PHOSPHATE).

Allergen Information:

CONTAINS WHEAT, COCONUT, MILK, AND SOY INGREDIENTS.

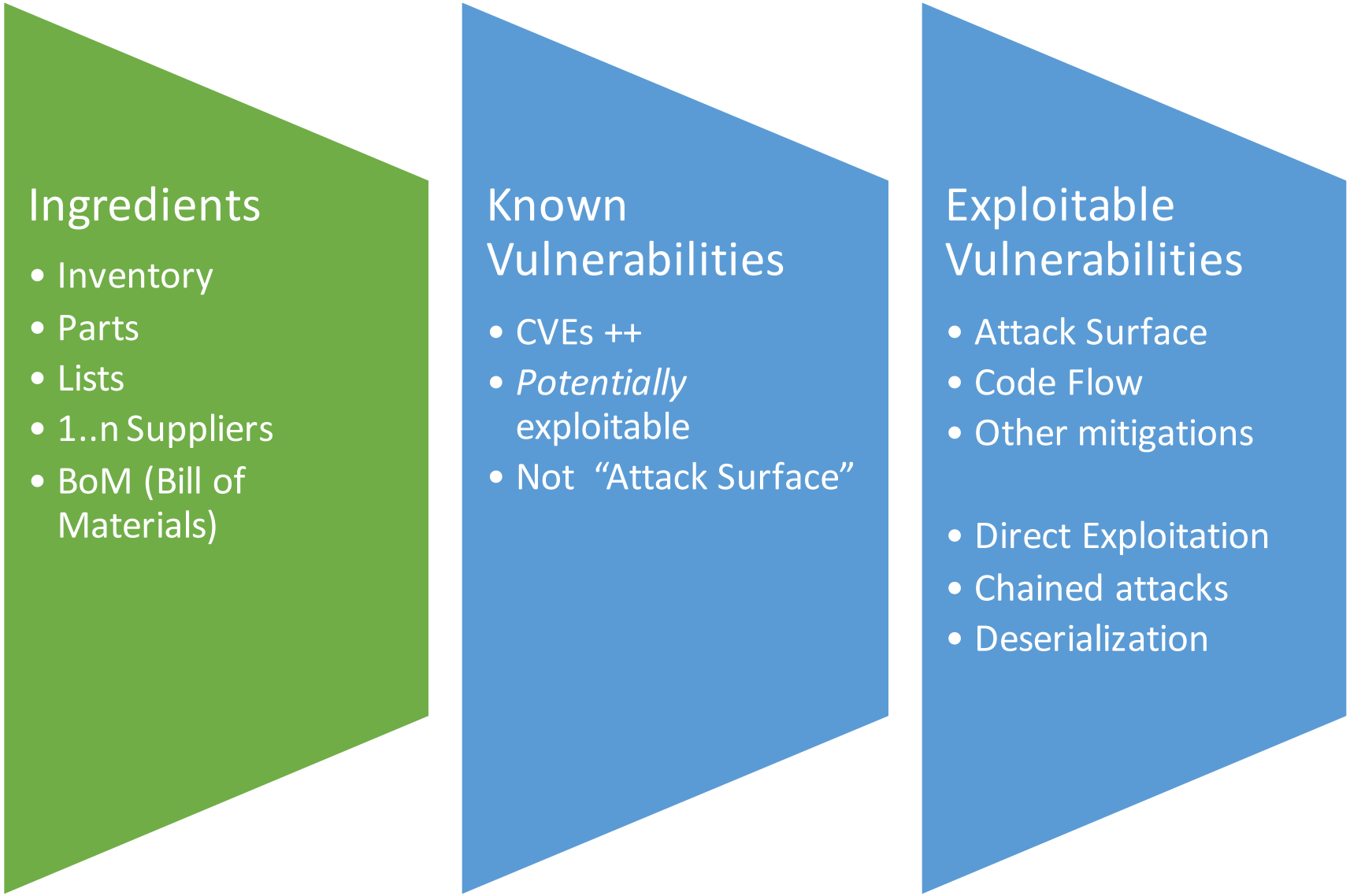


This document contains licenses and notices for open source software used in this product. With respect to the free/open source software listed in this document, if you have any questions or wish to receive a copy of any source code to which you may be entitled under the applicable free/open source license(s) (such as the GNU Lesser/General Public License), please contact us at external-opensource-requests@cisco.com.

In your requests please include the following reference number 78EE117C99-37892935

Contents

1.1 #ziplib? (SharpZipLib) 0.83


Ingredients
• Inventory
• Parts
• Lists
• 1..n Suppliers
• BoM (Bill of Materials)
Known Vulnerabilities
• CVEs ++
• *Potentially* exploitable
• Not "Attack Surface"
Exploitable Vulnerabilities
• Attack Surface
• Code Flow
• Other mitigations
• Direct Exploitation
• Chained attacks
• Deserialization


EMERGENCY

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

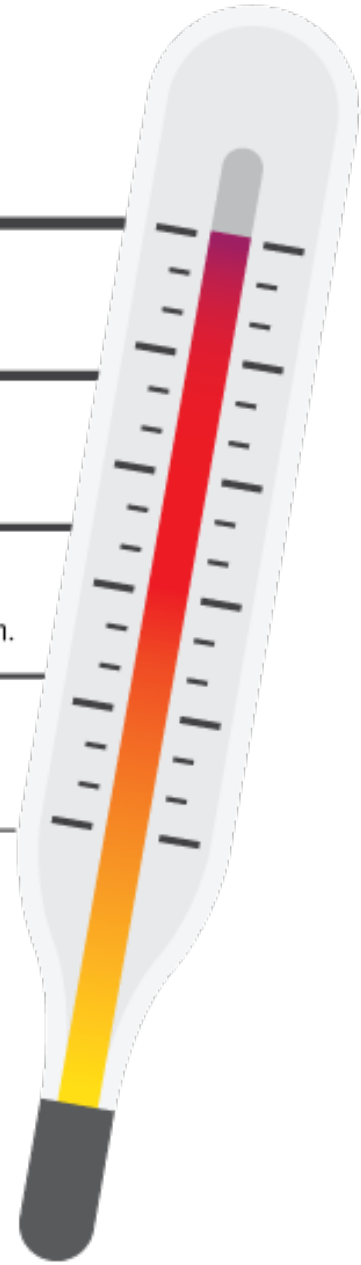
Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities




Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 14:57:41
Time Left
02:23:59:02
Your files will be lost on
5/19/2017 14:57:41
Time Left
06:23:59:02
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment

The NEW ENGLAND JOURNAL of MEDICINE

SPECIAL ARTICLE

Delays in Emergency Care and Mortality during Major U.S. Marathons

Anupam B. Jena, M.D., Ph.D., N. Clay Mann, Ph.D., Leia N. Wedlund, and Andrew Olenski, B.S.

ABSTRACT

BACKGROUND

Large marathons frequently involve widespread road closures and infrastructure disruptions, which may create delays in emergency care for nonparticipants with acute medical conditions who live in proximity to marathon routes.

SPECIAL ARTICLE

CONCLUSIONS

Medicare beneficiaries who were admitted to marathon-affected hospitals with acute myocardial infarction or cardiac arrest on marathon dates had longer ambulance transport times before noon (4.4 minutes longer) and higher 30-day mortality than beneficiaries who were hospitalized on nonmarathon dates. (Funded by the National Institutes of Health.)

ABSTRACT

BACKGROUND

Large marathons frequently involve widespread road closures and infrastructure disruptions, which may create delays in emergency care for nonparticipants with acute medical conditions who live in proximity to marathon routes.


EMERGENCY

Mostly Human: Hacker Down | ISIS' Twitter Star

The story of the first person deemed dangerous enough to kill... because of his ability to tweet. Watch the rest of the episodes on CNNgo via Apple TV, Roku, and Amazon Fire TV. Source: CNNMoney

Software Supply Chain Hygiene

Use better & fewer suppliers

Use higher quality parts

Track what you use and where

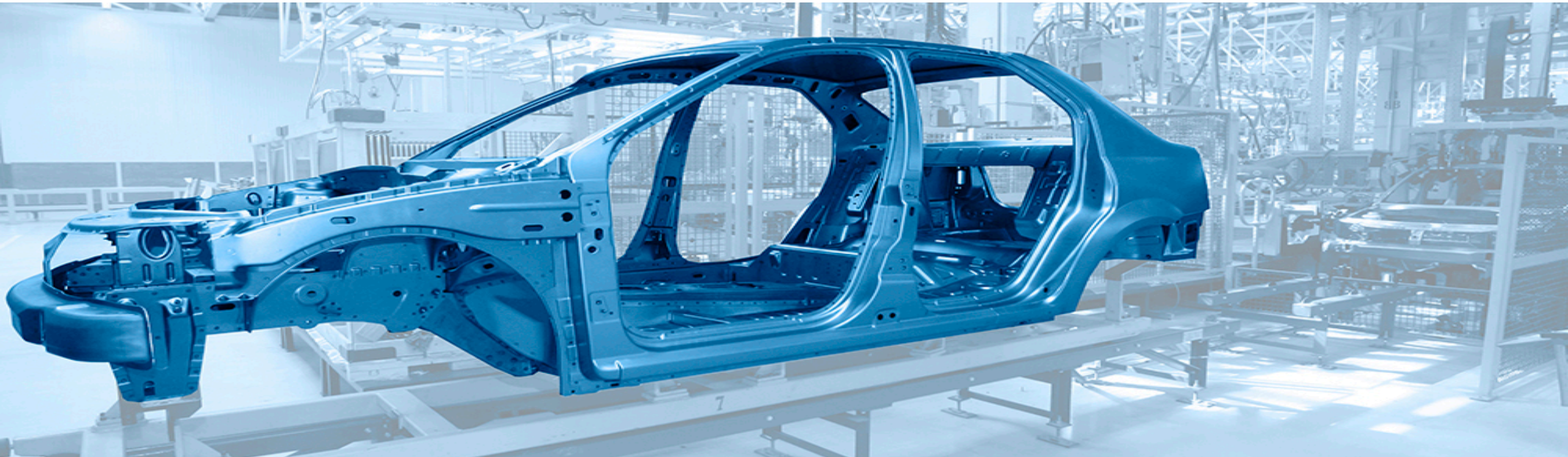
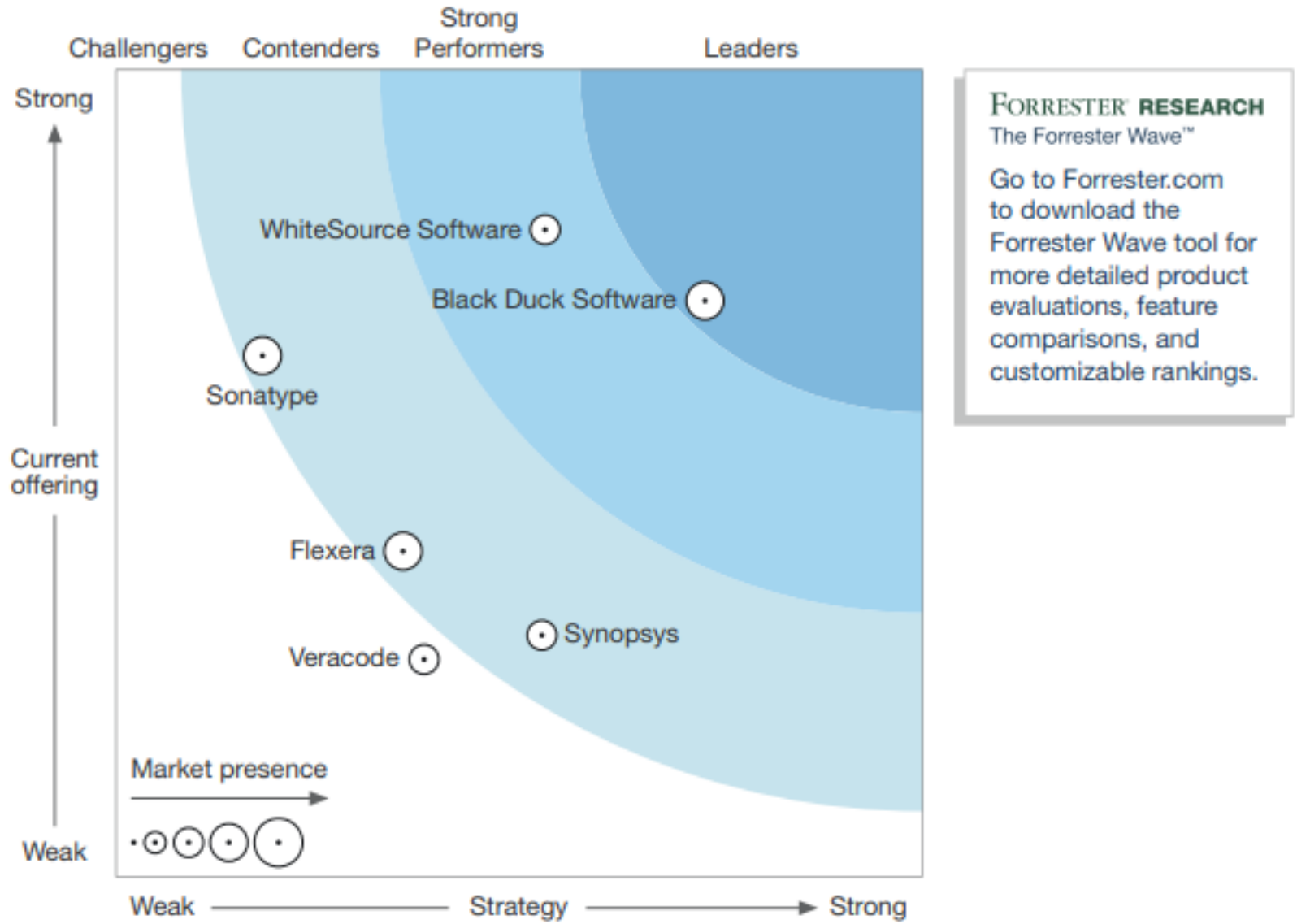


FIGURE 2 Forrester Wave™: Software Composition Analysis, Q1 '17



Sonatype Impact of software supply chain practices: Development Waste

Learn More Scenarios

Suppliers/ FOSS Projects 300

Versions / component 27

Known Undesir. % 90

8,100 versions; **7,290** undesirable; **106** components in use.

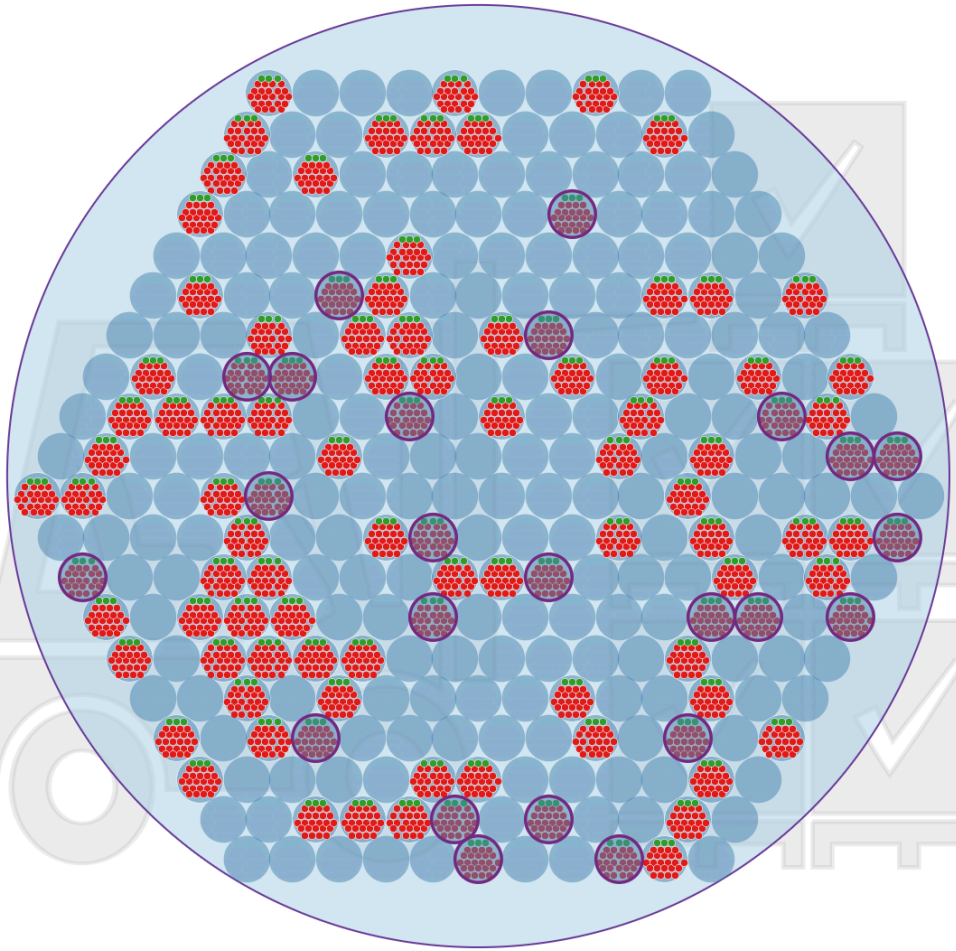
10,600 total components in use; **2,400** undesirable; including **848** with restrictive licenses

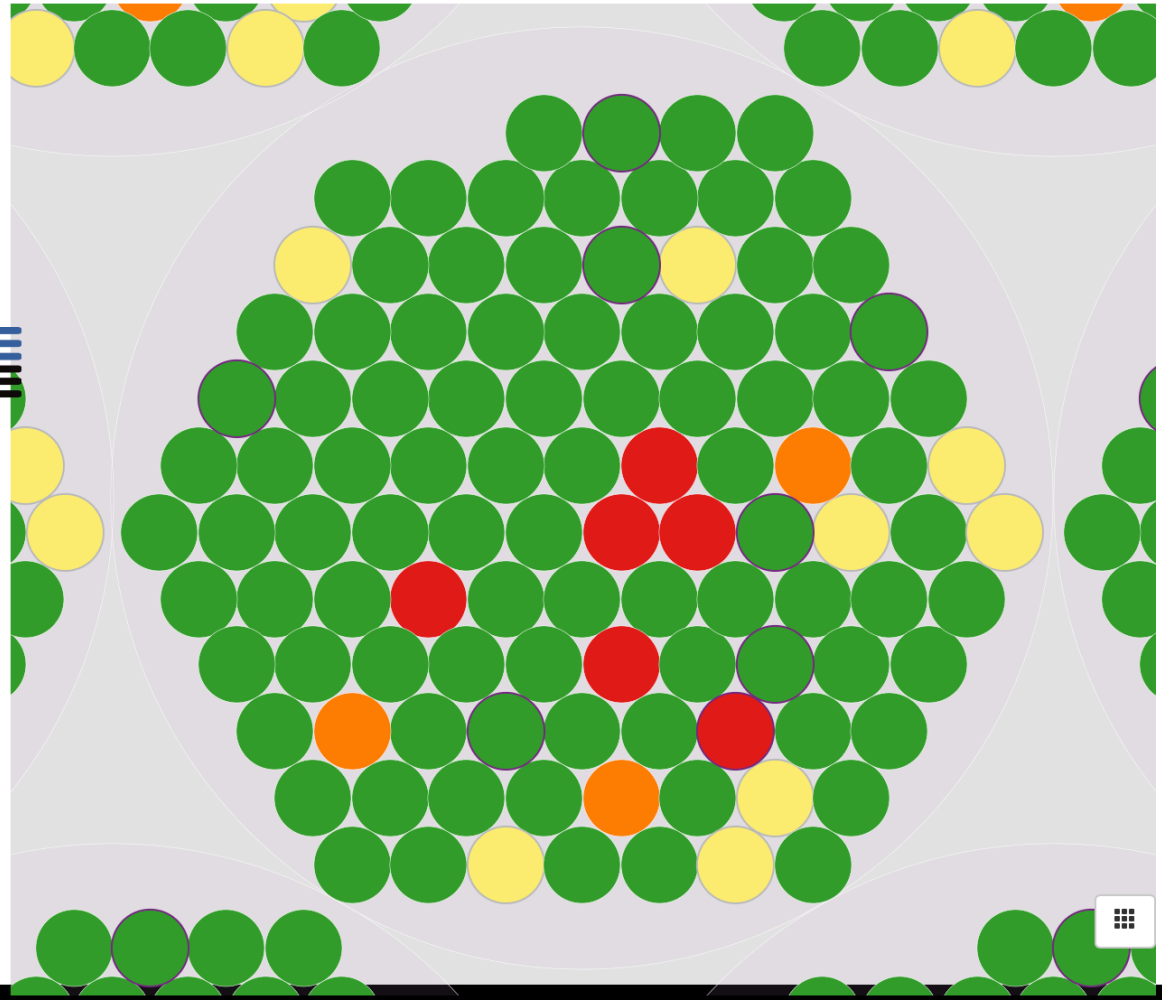
Number of Apps 100

Components per App 106

Vuln ratio % of parts 23

Restrictive licenses % 8





% Requiring Attention 10

Cost per hour 100 $

Unplanned work/fix (hrs) 10

240 components remediated out of **2,400**, requiring **2,400** hrs of effort to fix == **$240,000**USD

Calculations do not include **breach cost**, **help desk calls**, **maintenance**, **time-to-market**, **reputation** or **stock price**.

STRUTS2 - 2013

Global Bank

Software Provider

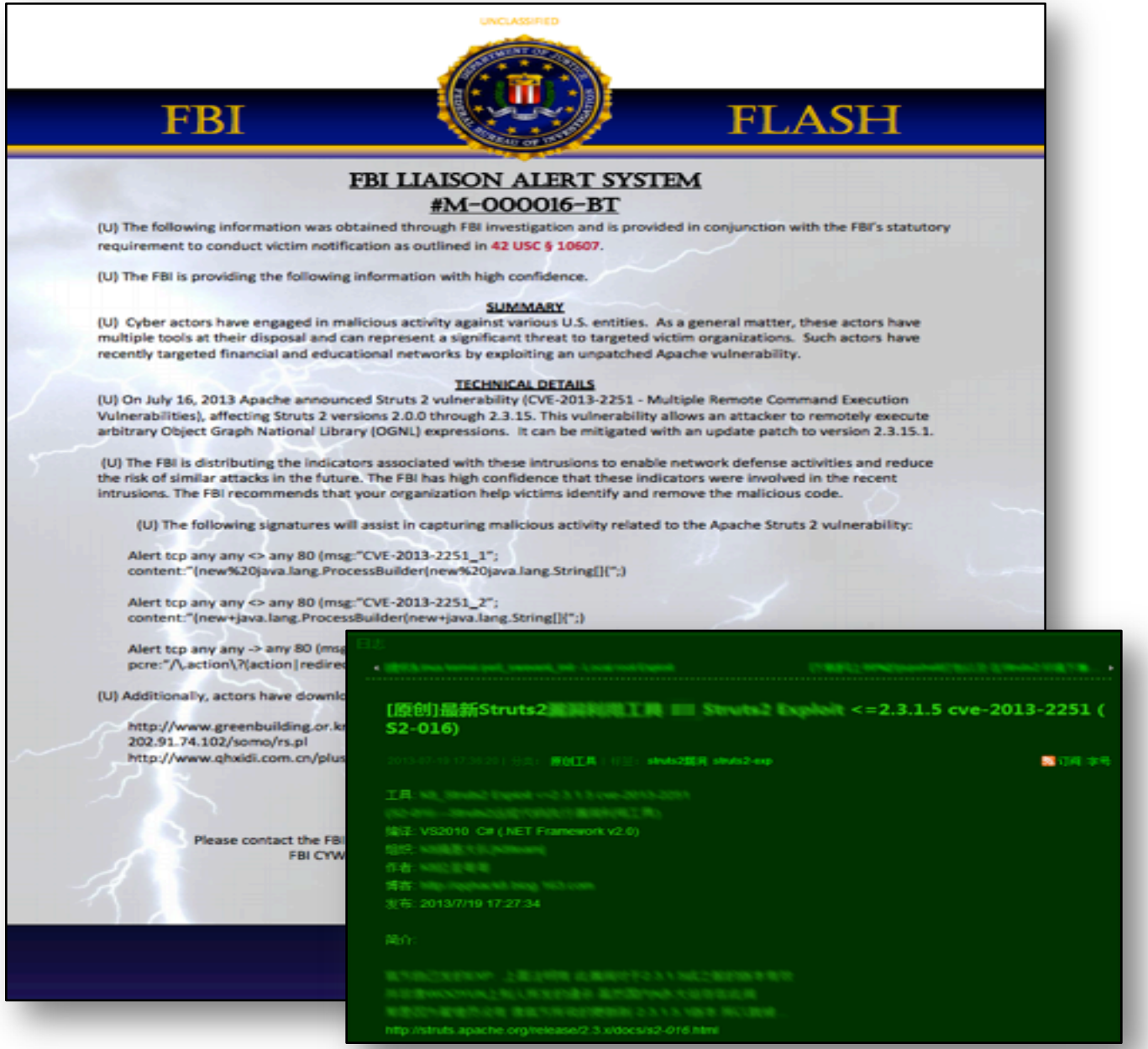
Software Provider's Customer

State University

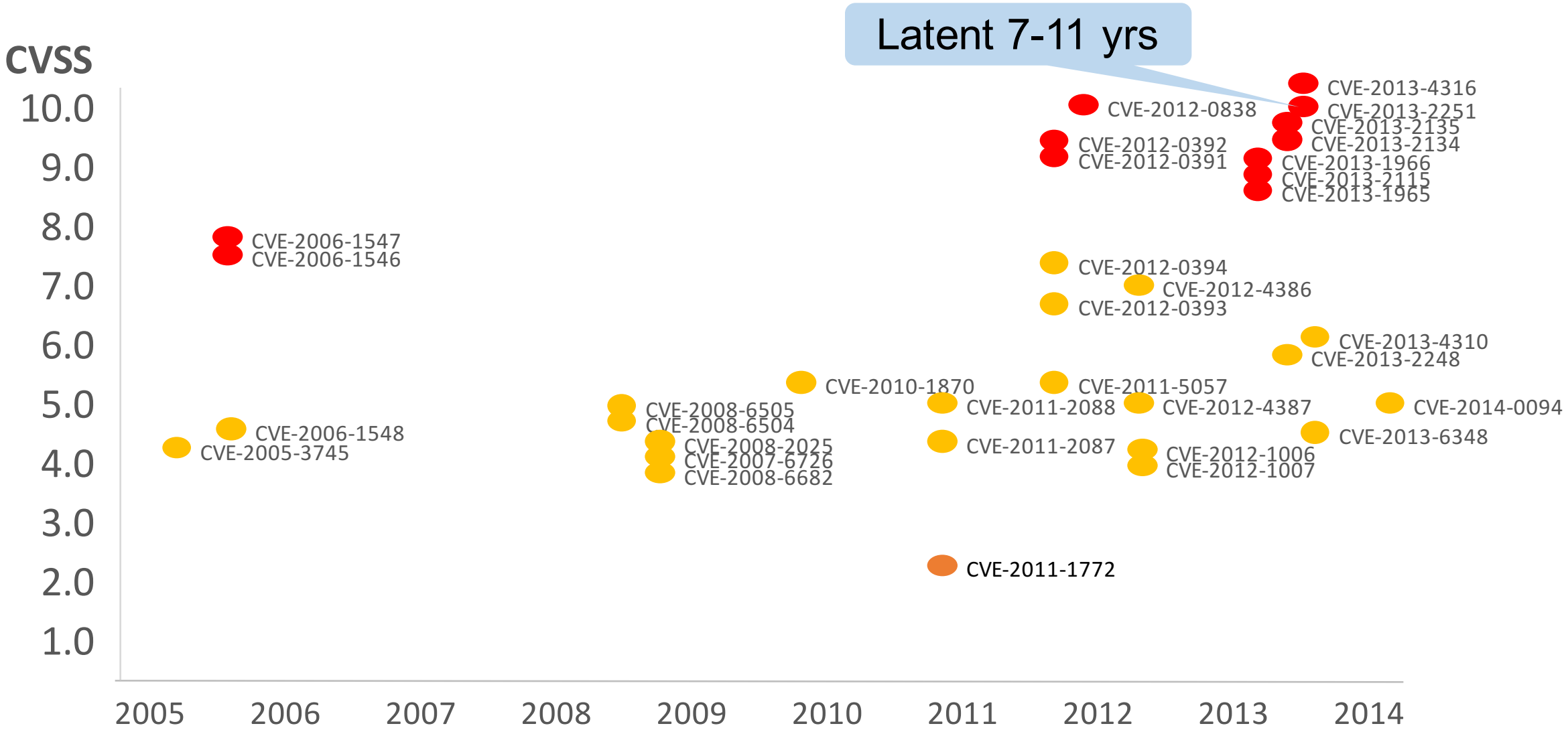
Three-Letter Agency

Large Financial Exchange

Hundreds of Other Sites



w/many eyeballs, all bugs are SHALLOW? Struts



COLUMNS

Almost Too Big to Fail

DAN GEER AND JOSHUA CORMAN

Dan Geer is the CISO for In-Q-Tel and a security researcher with a quantitative bent. He has a long history with the USENIX Association, including officer positions, program committees, etc. dan@geer.org

Joshua Corman is the chief technology officer for Sonatype. Previously, Corman served as a security researcher and strategist at Akamai Technologies, The 451 Group, and IBM Internet Security Systems. A respected innovator, he co-founded Rugged Software and I Am the Cavalry to encourage new security approaches in response to the world's increasing dependence on digital infrastructure. He is also an adjunct faculty for Carnegie Mellon's Heinze College, IANS Research, and a Fellow at the Ponemon Institute. Josh received his bachelor's degree in philosophy, graduating summa cum laude, from the University of New Hampshire. joshcorman@gmail.com

Both dependence on open source and adversary activity around open source are widespread and growing, but the dynamic pattern of use requires new means to estimate if not bound the security implications. In April and May 2014, every security writer has talked about whether it is indeed true that with enough eyeballs, all bugs are shallow. We won't revisit that topic because there may be no minds left to change. Unarguably:

- Dependence on open source is growing in volume and variety.
- Adversary interest tracks installed base.
- Multiple levels of abstraction add noise to remediation needs.

We begin with two open source examples.

Apache Struts CVE-2013-2251, July 6, 2013 - CVSS v2 9.3

Apache Struts is one of the most popular and widely depended upon open source projects in the world. As such, when this highly exploitable vulnerability was discovered, it was promptly used to compromise large swaths of the financial services sector. While Heartbleed (see below) got full media frenzy, many affected by 2013-2251 learned of the problem from FBI victim notifications under 42 U.S.C. § 10607. The FS-ISAC issued guidance [1] telling institutions (read, victims) to scrutinize the security of third-party and open source components throughout their life cycle of use. It is not noteworthy that an open source project could have a severe vulnerability; what is of note is that this flaw went undetected for at least seven years (if not a lot longer from WebWork 2/pre-Struts 2 code base)—an existence proof that well-vetted code still needs a backup plan.

OpenSSL (Heartbleed) CVE-2014-0160, April 7, 2014 - CVSS v2 5.0

The Heartbleed vulnerability in OpenSSL garnered tremendous media and attacker activity this past April. While only scored with a CVSS of 5.0, it is a "5 with the power of a 10" since sniffing usernames, passwords, and SSL Certificates provides stepping stones to far greater impact. In contrast to the Struts bug above, this flaw was introduced only two years prior, but it, too, went unnoticed by many eyeballs—it was found by bench analysis [2].

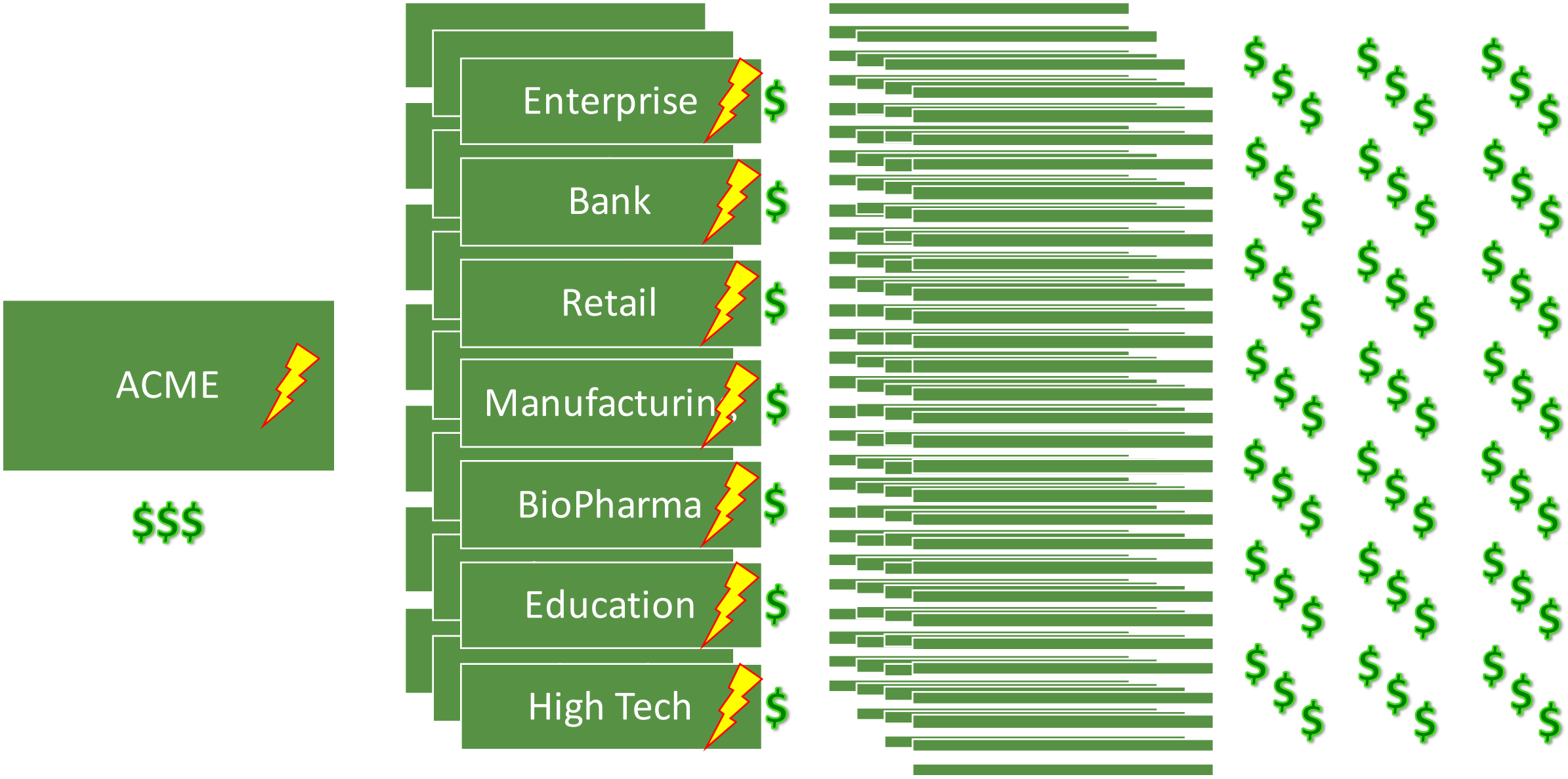
Dependence on Open Source Is Growing

Sonatype, home to author Corman, serves as custodian to Central Repository, the largest parts warehouse in the world for open source components. At the macro level, open source consumption is exploding in Web applications, mobility, cloud, etc., driven in part by increasingly favorable economics. Even (risk averse, highly regulated) government and financial sectors, which previously resisted "code of unknown origin/quality/security," have begun relaxing their resistance. According to both Gartner surveys and Sonatype application analysis, 90+% of modern applications are not so much written as assembled from third-party building blocks. It is the open source building blocks that are taking the field, and not just for commodity applications (see Figure 1).

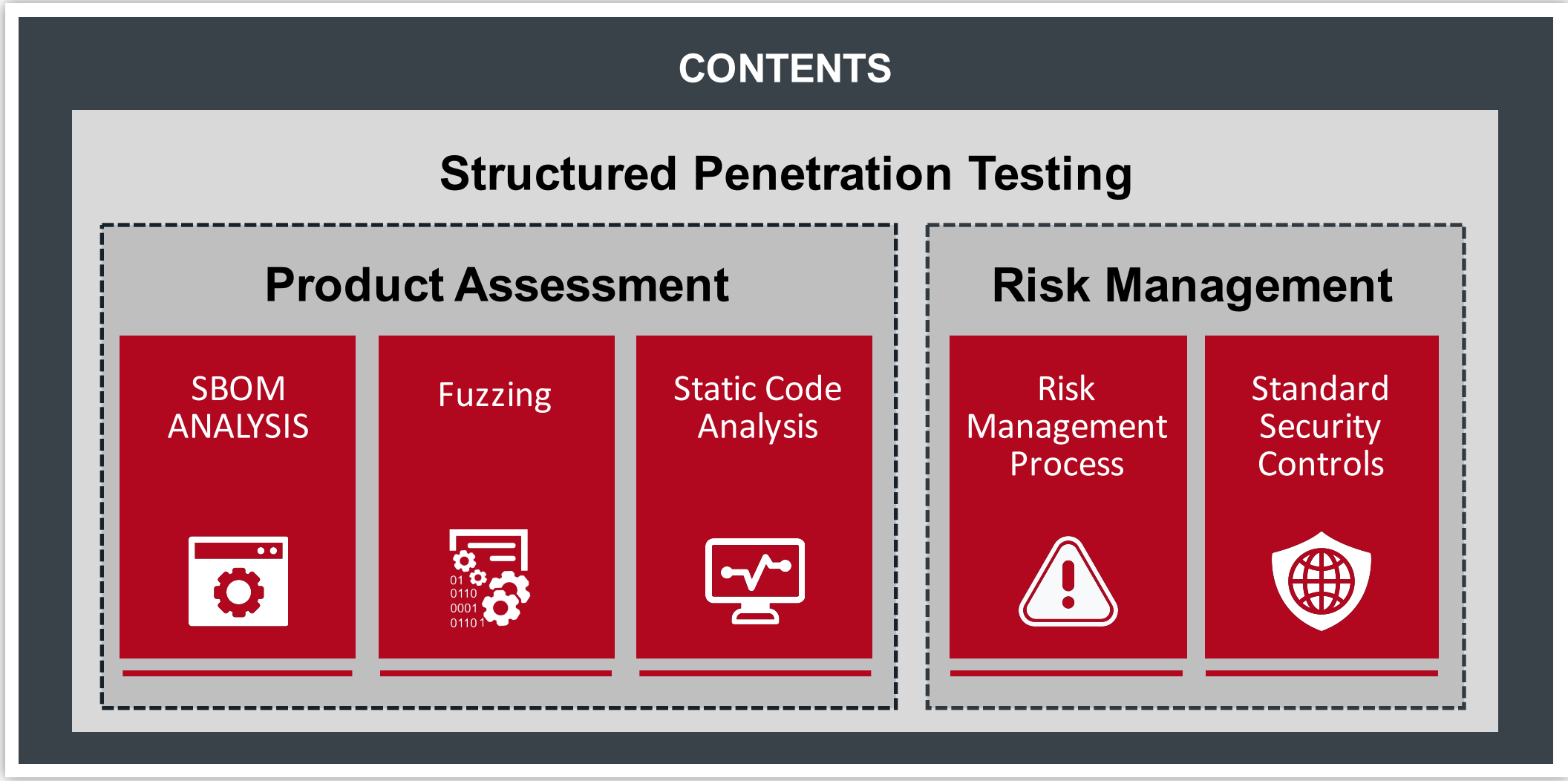
For the 41%
390 days
CVSS 10s 224 days

https://www.usenix.org/system/files/login/articles/15_geer_0.pdf

TRUE COSTS (& LEAST COST AVOIDERS)



UL 2900 primary contents



Government has noticed in the last 3 years*…

Presidential Commission Report

DOC/NTIA Guidance

FDA Guidance

DOJ Work Group

DOD Strategy

EU Guidance

DHS Guidance

FTC Guidelines

HHS Task Force

DOT Principles

NHTSA Guidance

Food and Drug Administration

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research

Department of Homeland Security

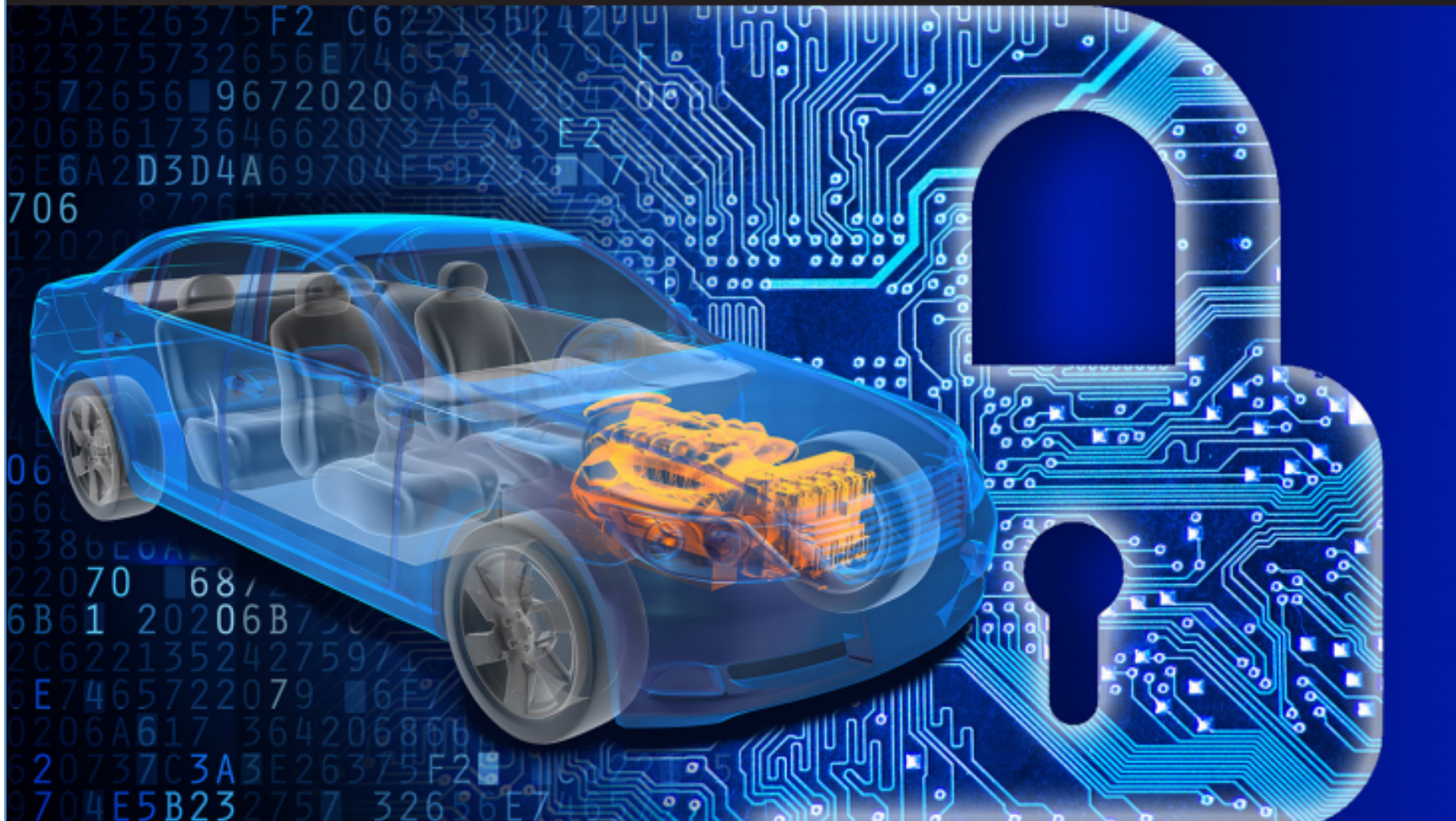
STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)

Version 1.0

November 15, 2016

Department of Transportation

Cybersecurity Best Practices for Modern Vehicles



Department of Commerce

Multistakeholder Process: Cybersecurity Vulnerabilities

Stakeholder documents

- Deputy Assistant Secretary Angela Simpson's blog post announcing the release of these documents
- Vulnerability Disclosure Attitudes and Actions: A Research Report
- Coordinated Vulnerability Disclosure "Early Stage" Template
- Guidelines and Practices for Multi-party Vulnerability Coordination

Vulnerability Disclosure Attitudes and Actions

A Research Report from the NTIA Awareness and Adoption Group

"Early Stage"
Coordinated Vulnerability Disclosure Template
Version 1.1[1]

NTIA Safety Working Group
December 15, 2016

Presidential Commission Report

COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

DECEMBER 1, 2016

REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY

Presidential Commission Report

Action Item 3.1.1: *To improve consumers' purchasing decisions, an independent organization should develop the equivalent of a cybersecurity "nutritional label" for technology products and services—ideally linked to a rating system of understandable, impartial, third-party assessment that consumers will intuitively trust and understand.* (SHORT AND MEDIUM TERM)

(ii) The executive branch has for too long accepted antiquated and difficult-to-defend IT.

(iii) Effective risk management involves more than just protecting IT and data currently in place. It also requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity.

(iv) Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies (agencies). Known vulnerabilities include using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security-specific configuration guidance.

Scott Gottlieb, M.D. ✓
@SGottliebFDA

THREAD: We're proud to work with the public-private Healthcare Sector Coordinating Council's Medical Technology & Health IT Task Group to address @HHSgov Cybersecurity Task Force Report recommendations related to medical device cybersecurity: healthsectorcouncil.org/health-sector-...

12:42 PM · Jul 18, 2018

17 Retweets **18** Likes

Scott Gottlieb, M.D. ✓ @SGottliebFDA · 19h
Replying to @SGottliebFDA
HSCC announced today a new workstream, conducted under the Task Group, that will discuss and seek input on a software bill of materials (SBOM) for medical devices. SBOMs can ensure that users have better understanding of what software elements are in a medical device.

1 6 7

Scott Gottlieb, M.D. ✓ @SGottliebFDA · 19h
Knowing what software is included in a device means users and manufacturers can better assess and remediate potential cybersecurity threats that may emerge. #FDA looks forward to participating in the SBOM workstream and engaging broader perspective from the community.

6 9

HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership

Home About Resources Contact

Health Sector Mobilizes Against Cyber Threats

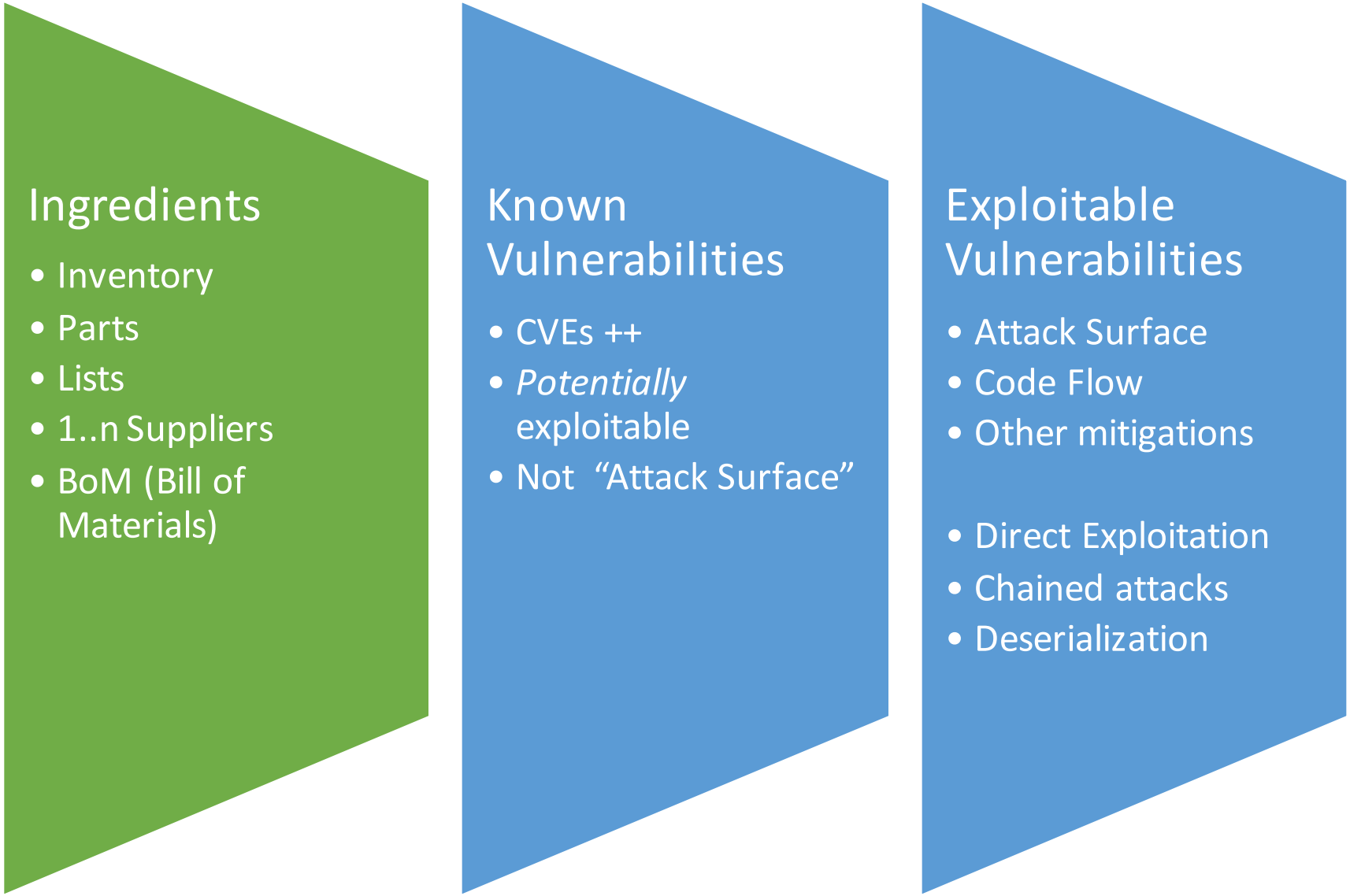
June 29 Health Sector Council Meeting in Washington gathers 120 industry and government leaders to meet the threat

Washington, DC – July xy - More than 100 healthcare providers, associations, pharmaceutical, medical device and health IT companies met with government officials in Washington DC June 29 to report and build on their collective progress toward implementing stronger cyber security protections across the healthcare sector. Executives met under the umbrella of the Healthcare and Public Health Sector Coordinating Council (HSCC), established under presidential executive order to identify and mitigate sector-wide threats and vulnerabilities against the delivery of healthcare services and assets.

The HSCC Joint Cybersecurity Working Group (JCWG) – composed of industry and government organizations - reorganized at the beginning of the year to respond to wide-ranging recommendations made by the 2017 Health Care Industry Cybersecurity Task Force (HCIC), an

VIEW ALL NEWS

- Health Sector Mobil Threats
  July 16, 2018
- Hacking Healthcare
  July 13, 2018
- The Healthcare Sect and the NH-ISAC: T Critical Infrastructu
  March 14, 2018


Ingredients
• Inventory
• Parts
• Lists
• 1..n Suppliers
• BoM (Bill of Materials)
Known Vulnerabilities
• CVEs ++
• *Potentially* exploitable
• Not "Attack Surface"
Exploitable Vulnerabilities
• Attack Surface
• Code Flow
• Other mitigations
• Direct Exploitation
• Chained attacks
• Deserialization

Now what…

- SBoM is happening…
  - Financial Services
  - HHS Action
  - Private sector procurement
  - …
- Can we ensure it is done…
  - Better
  - More consistently across sectors

Workstreams?

- Facts/Fiction/Common Objections/FAQ
- 80/20 “scope” across verticals ands use cases
- Machine Readable Format
- Persistent Triage of “Residuals” across stakeholders and time
- Fuller list of stakeholders and use cases
  - Builders/Suppliers
  - Saas
  - Procurement
  - Operational Hygiene
  - Post – “Out of Business”
- Collect and compare available data – toward more ground truth
- Known Vulnerability / CVE “challenges”

*Through our **over dependence** on **undependable IT**, we have created the conditions such that the actions **any single outlier** can have a profound and asymmetric impact on **human life, economic, and national security**.*


"SUNLIGHT IS SAID TO BE,
THE BEST OF DISINFECTANTS"
imgflip.com

Safer | Sooner | Together

@joshcorman

@IamTheCavalry

I am The Cavalry