Software Bill of Materials (SBOM) Primer

Joshua Corman
@joshcorman

NTIA Supply Chain Transparency
07/19/2018
Where Bits & Bytes meet Flesh & Blood
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.

<table>
<thead>
<tr>
<th>Nutrition Facts</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 servings per container</td>
</tr>
</tbody>
</table>

| Serving size | 1 cup (140g) |

| Amount per serving | Calories: 160 |

<table>
<thead>
<tr>
<th>% Daily Value*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Fat 9g</td>
</tr>
<tr>
<td>Saturated Fat 3g</td>
</tr>
<tr>
<td>Cholesterol 0mg</td>
</tr>
<tr>
<td>Sodium 50mg</td>
</tr>
<tr>
<td>Total Carbohydrate 21g</td>
</tr>
<tr>
<td>Dietary Fiber 3g</td>
</tr>
<tr>
<td>Total Sugars 15g</td>
</tr>
<tr>
<td>Includes 5g Added Sugars</td>
</tr>
<tr>
<td>Protein 3g</td>
</tr>
</tbody>
</table>

At least 10-point **bold** or **extra-bold**; amount must be right-justified.

At least 22-point **bold** or **extra-bold**.

At least 8-point. Nutrients that are not indented (Total Fat, Cholesterol, etc.) should be flush left and **bold** or **extra-bold**.

At least 8-point. **Vitamin D** 5mcg 25%

**Calcium** 200mg 2%

**Iron** 1mg 6%

**Potassium** 230mg 4%

*The % Daily Value tells you how much a nutrient in a serving of a food contributes to a daily diet. 2,000 calories a day is used for general nutrition advice.

© 2016 ESHA Research
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
   1.1.1 Available under license
1.2 ACE 5.3
   1.2.1 Available under license
1.3 ActiveMQ 5.3.1
   1.3.1 Available under license
1.4 AmazonS3 2011-01-22
   1.4.1 Available under license
1.5 ant 1.7.1
   1.5.1 Available under license

1.103.2 Available under license
1.104 xerces java parser 2.6.2
   1.104.1 Notifications
   1.104.2 Available under license
1.105 xml-apis 1.4.01
   1.105.1 Available under license
1.106 xpp3 1.1.3.8 :1.jpp5
   1.106.1 Notifications
   1.106.2 Available under license
1.107 zlib 1.2.3
   1.107.1 Available under license
**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
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!

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 GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

Contact Us

About bitcoin
How to buy bitcoins?
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.
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.
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
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

Latent 7-11 yrs
For the 41%
390 days
CVSS 10s 224 days
TRUE COSTS (& LEAST COST AVOIDERS)

- Enterprise
- Bank
- Retail
- Manufacturing
- BioPharma
- Education
- High Tech

ACME $$$$
UL 2900 primary contents

CONTENTS

Structured Penetration Testing

Product Assessment
- SBOM ANALYSIS
- Fuzzing
- Static Code Analysis

Risk Management
- Risk Management Process
- Standard Security Controls
Government has noticed in the last 3 years*...

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DHS Guidance</td>
<td>FTC Guidelines</td>
<td>HHS Task Force</td>
<td>DOT Principles</td>
<td>NHTSA Guidance</td>
<td></td>
</tr>
</tbody>
</table>
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.
STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)
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

NTIA Safety Working Group
December 15, 2016
COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

DECEMBER 1, 2016

REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY
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.
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

HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership

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 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
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 and 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"
Safer | Sooner | Together

@joshcorman
@IamTheCavalry

I am The Cavalry