DevSecOps Day EMEA

Unlock 2024

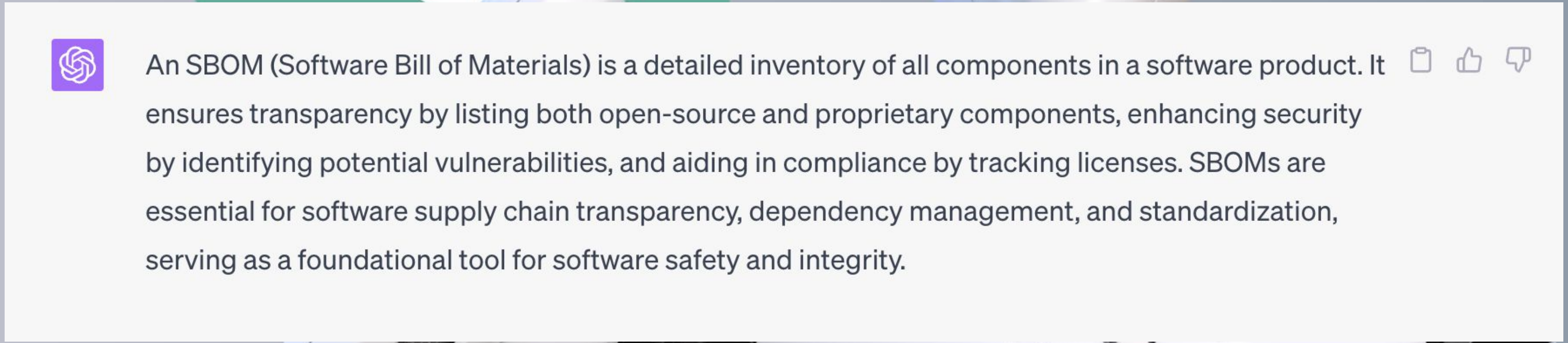
SBOM

IS NOT A FOUR LETTER WORD

Bill Manning, Solutions Engineering Manager

@williammanning

WHAT IS AN SBOM?

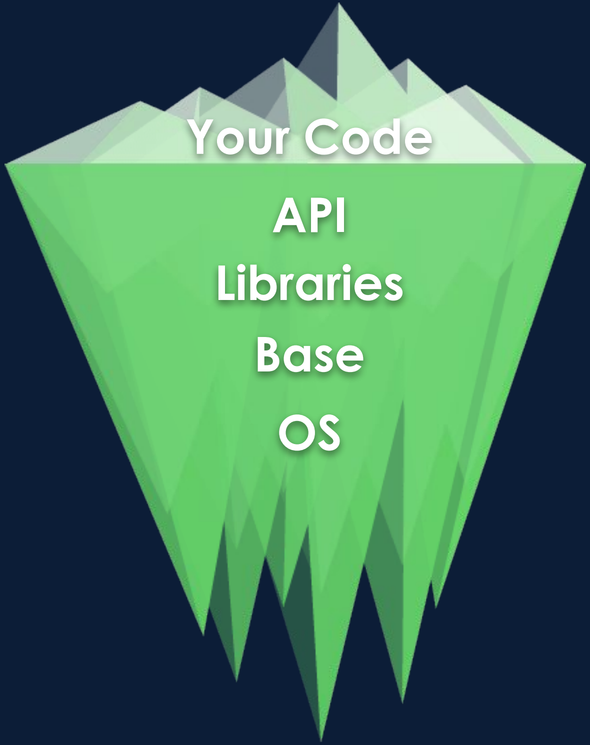


An SBOM (Software Bill of Materials) is a detailed inventory of all components in a software product. It ensures transparency by listing both open-source and proprietary components, enhancing security by identifying potential vulnerabilities, and aiding in compliance by tracking licenses. SBOMs are essential for software supply chain transparency, dependency management, and standardization, serving as a foundational tool for software safety and integrity.

WHY SBOM?

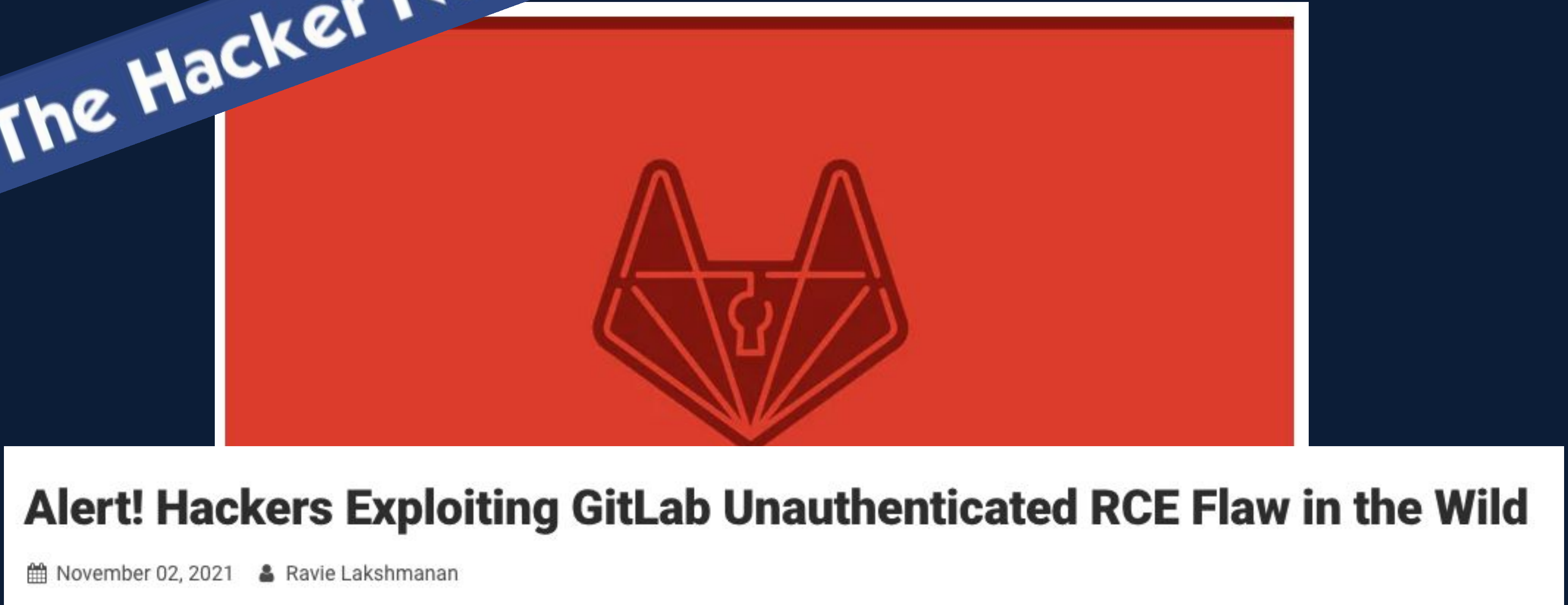
OPEN SOURCE & COMPLIANCE

Most software is composed of 85-90% open source components



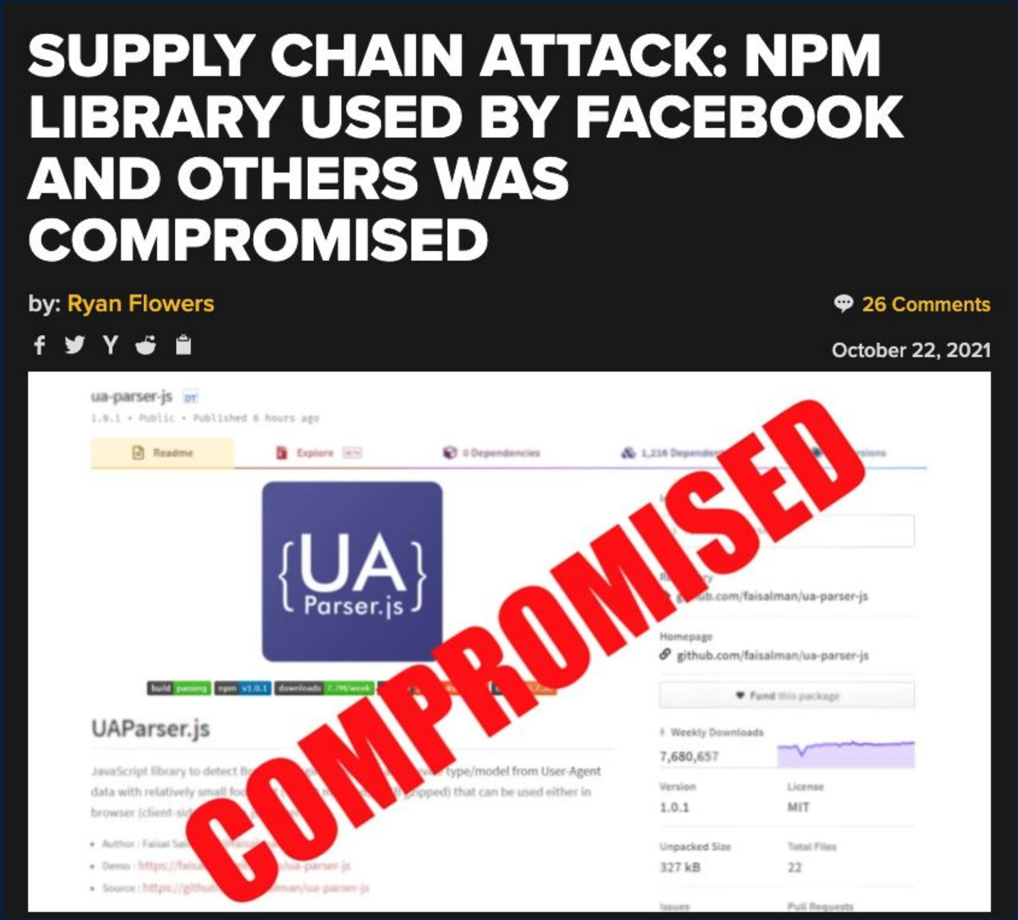
Every time you **pip install**, **go get**, or **mvn fetch** something, you’re doing the equivalent of plugging a thumb drive you found on the sidewalk into your production server.

The Hacker News



Alert! Hackers Exploiting GitLab Unauthenticated RCE Flaw in the Wild

November 02, 2021 Ravie Lakshmanan



SUPPLY CHAIN ATTACK: NPM LIBRARY USED BY FACEBOOK AND OTHERS WAS COMPROMISED

by: Ryan Flowers

26 Comments

October 22, 2021

ua-parser-js DT

1.0.1 • Public • Published 6 hours ago

UAParser.js

JavaScript library to detect B[...] type/model from User-Agent data with relatively small foo[...] gzipped) that can be used either in browser (client-sid

- Author : Faisal Sa
- Demo : https://faisa /ua-parser-js
- Source : https://github man/ua-parser-js

Repository
github.com/faisalman/ua-parser-js

Homepage
github.com/faisalman/ua-parser-js

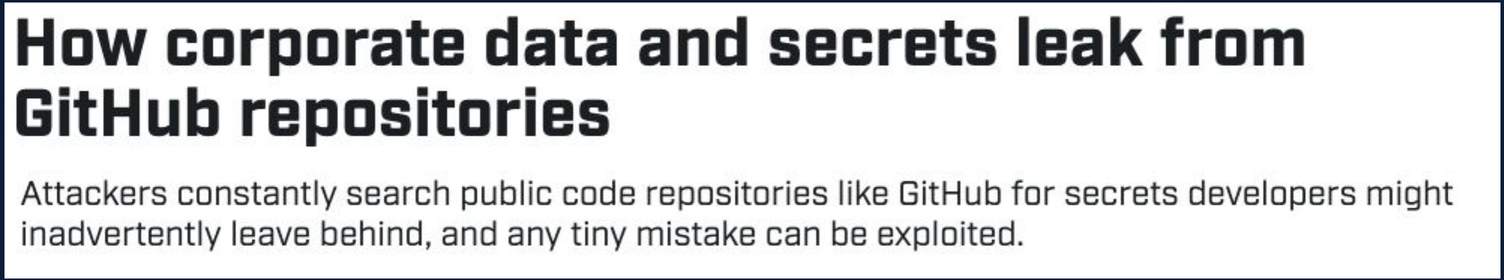
Fund this package

Weekly Downloads
7,680,657

Version	License
1.0.1	MIT

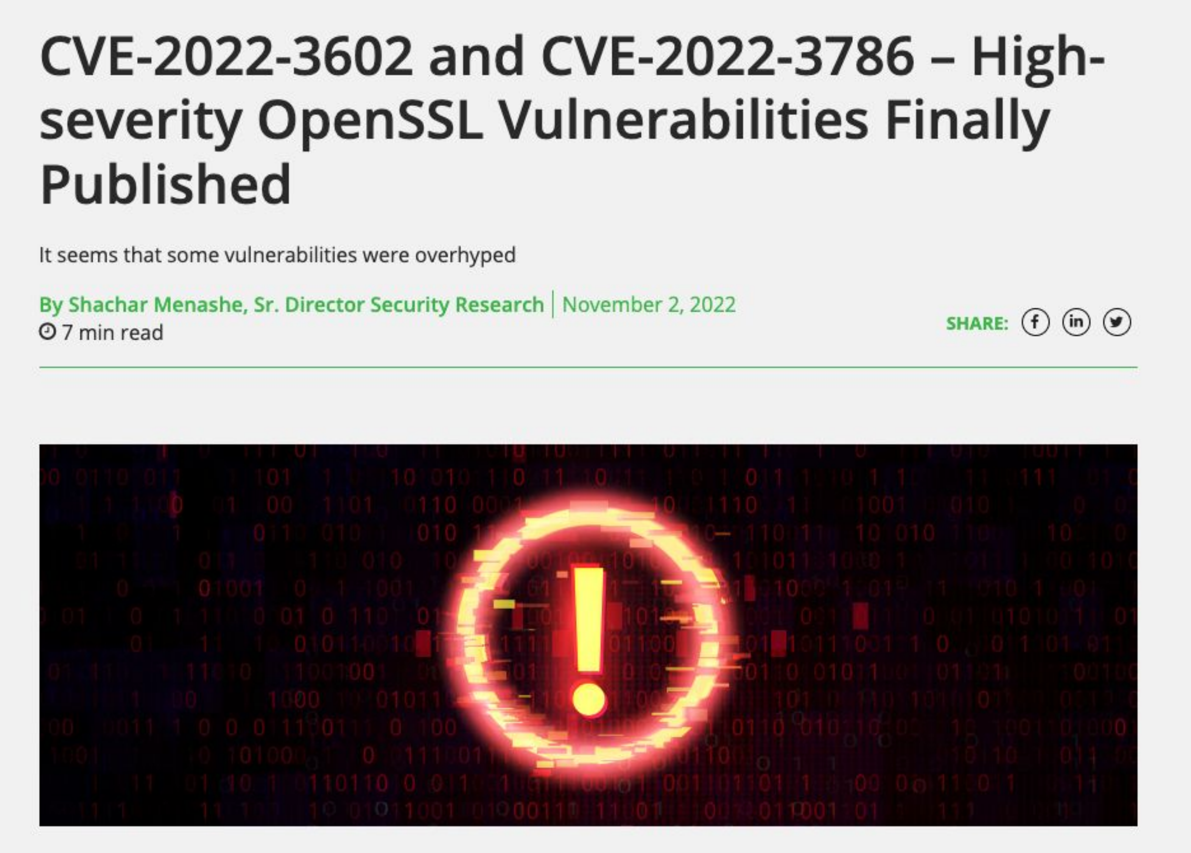
Unpacked Size	Total Files
327 kB	22

Issues Pull Requests



How corporate data and secrets leak from GitHub repositories

Attackers constantly search public code repositories like GitHub for secrets developers might inadvertently leave behind, and any tiny mistake can be exploited.



CVE-2022-3602 and CVE-2022-3786 – High-severity OpenSSL Vulnerabilities Finally Published

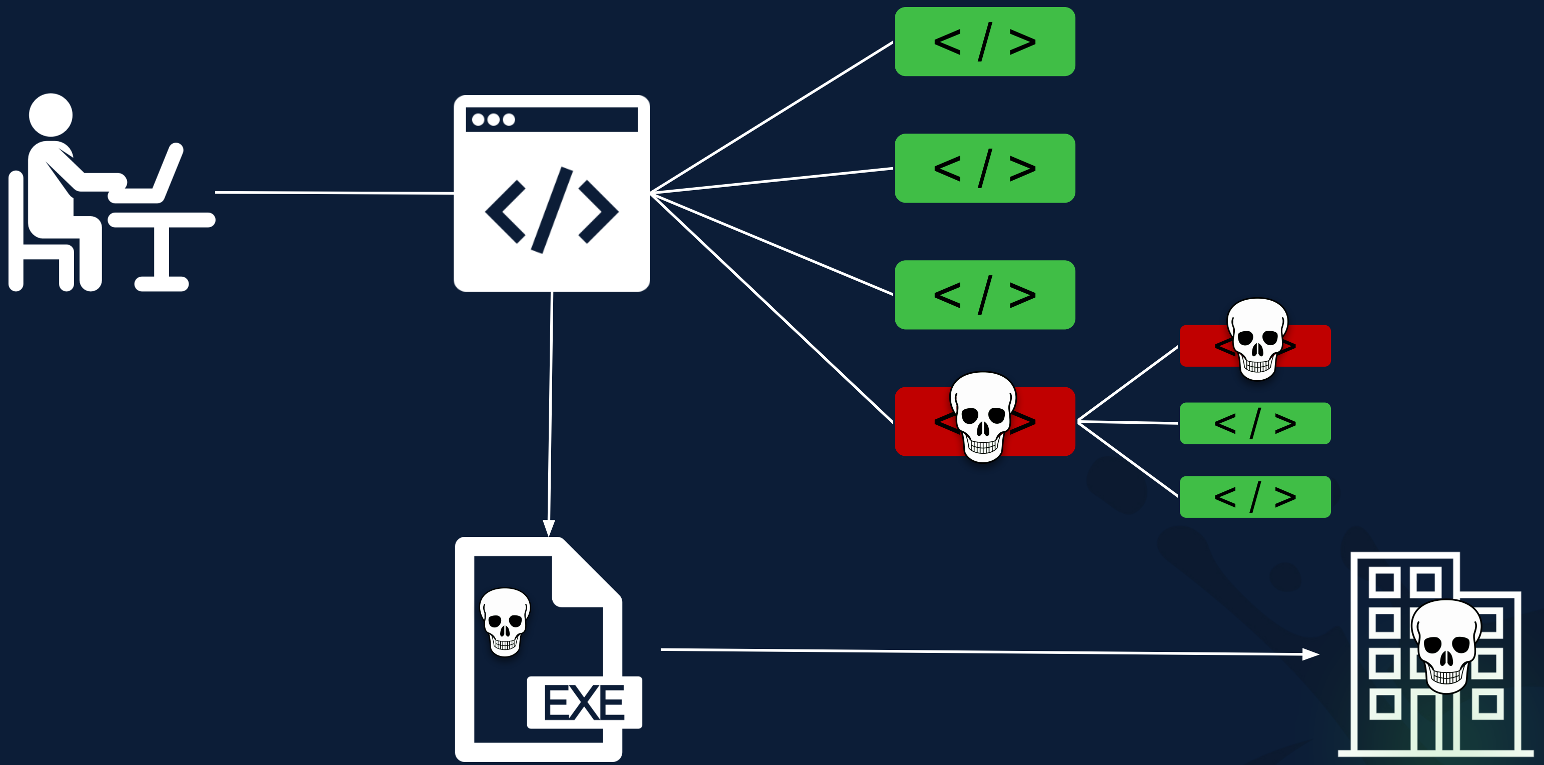
It seems that some vulnerabilities were overhyped

By Shachar Menashe, Sr. Director Security Research | November 2, 2022

7 min read

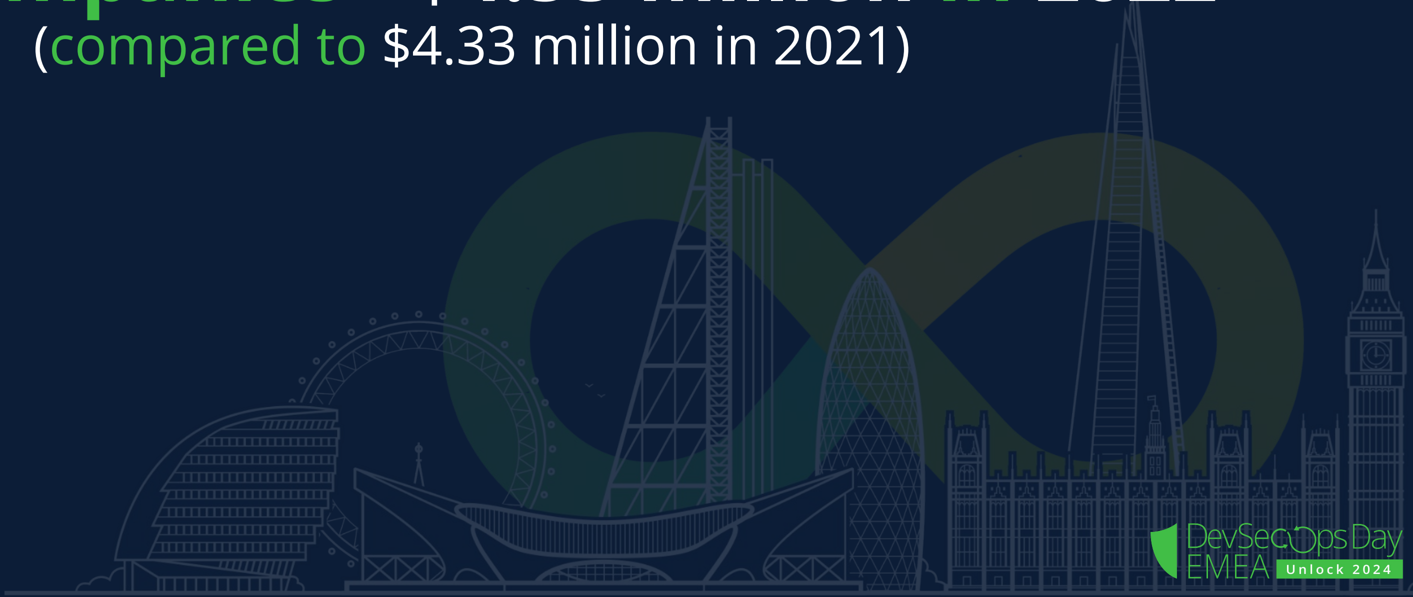
SHARE:

HOW DO ATTACKS OCCUR?



Vulnerabilities in third-party software cost companies - $4.55 million in 2022

(compared to $4.33 million in 2021)



Almost 21,000 CVEs were registered in 2022

99% of all software developed and **85%** of enterprise software has open-source components

62% of all attacks exploited supplier trust and attacks have increased 6.5x from 2015 to 2021

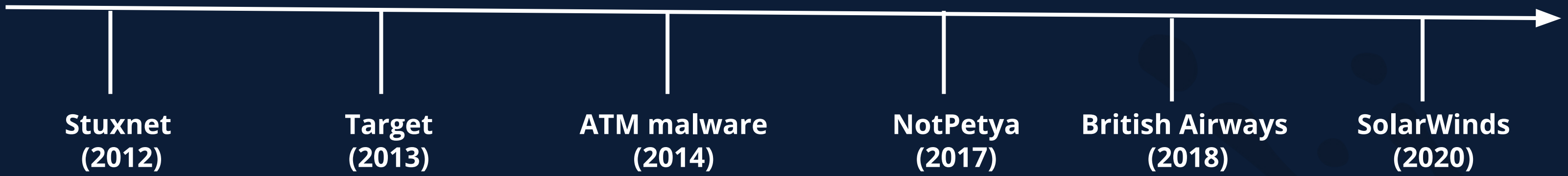
Attacks are estimated to grow by **4X** YoY in 2022

Supplier breaches are **10X** more expensive than 1st and 2nd party

SOFTWARE SUPPLY CHAIN ATTACKS

The definition we all know:

A technique in which an adversary slips malicious code or even a malicious component into a trusted piece of software or hardware.



Stuxnet (2012)

Target (2013)

ATM malware (2014)

NotPetya (2017)

British Airways (2018)

SolarWinds (2020)

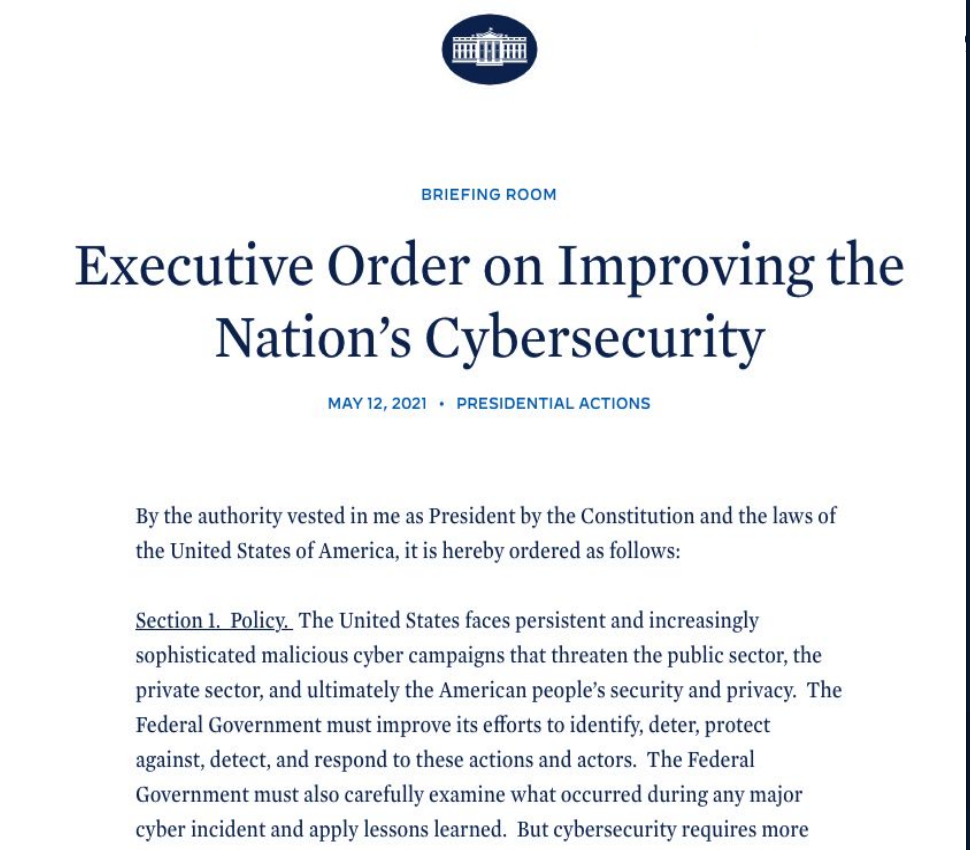
solarwinds

"Eighteen thousand [customers] was our best estimate of who may have downloaded the code between March and June of 2020."

Sudhakar Ramakrishna, SolarWinds President & CEO

MAY 12TH, 2021

The United States Government equates cybersecurity with national security.



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

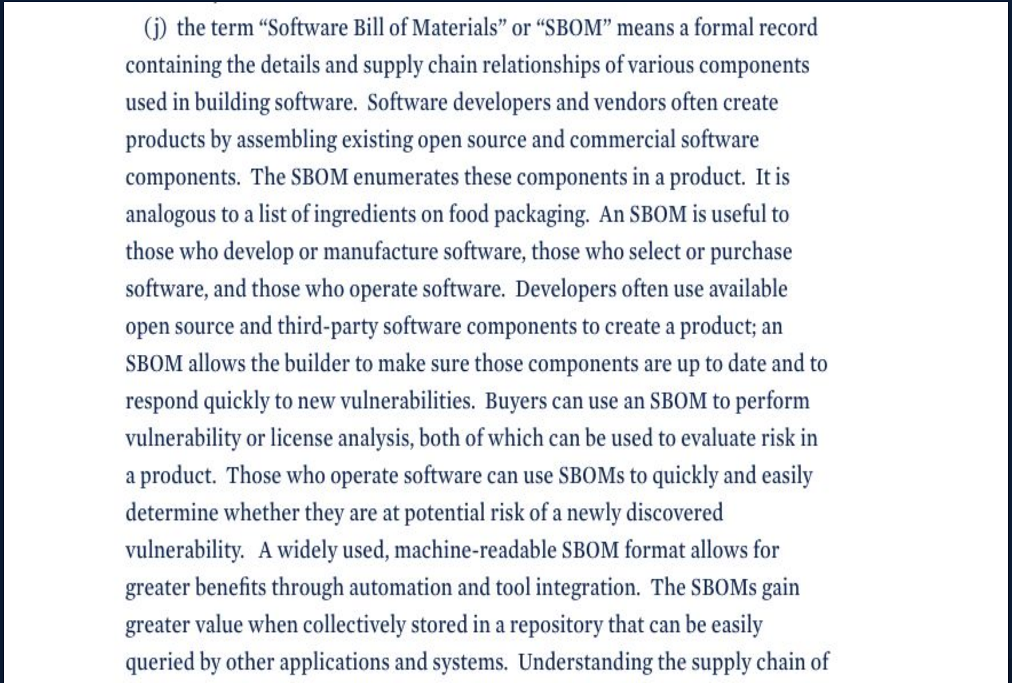
MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

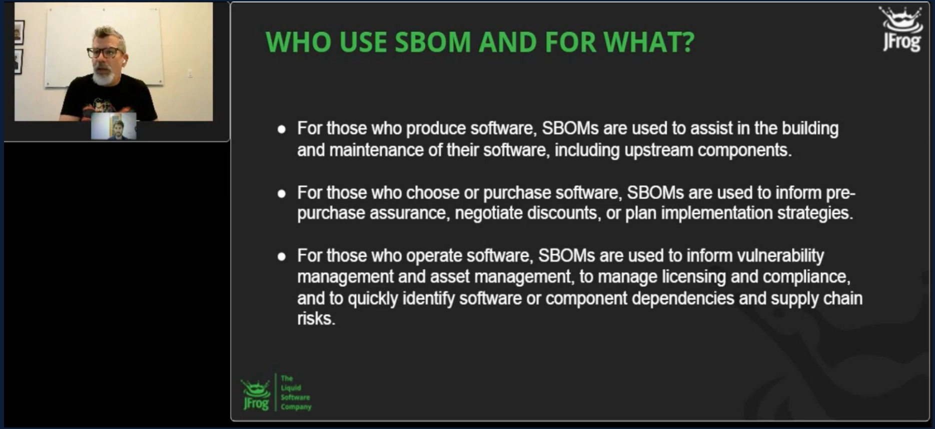
Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more

Sec. 4. Enhancing Software Supply Chain Security

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;



(j) the term “Software Bill of Materials” or “SBOM” means a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product. It is analogous to a list of ingredients on food packaging. An SBOM is useful to those who develop or manufacture software, those who select or purchase software, and those who operate software. Developers often use available open source and third-party software components to create a product; an SBOM allows the builder to make sure those components are up to date and to respond quickly to new vulnerabilities. Buyers can use an SBOM to perform vulnerability or license analysis, both of which can be used to evaluate risk in a product. Those who operate software can use SBOMs to quickly and easily determine whether they are at potential risk of a newly discovered vulnerability. A widely used, machine-readable SBOM format allows for greater benefits through automation and tool integration. The SBOMs gain greater value when collectively stored in a repository that can be easily queried by other applications and systems. Understanding the supply chain of



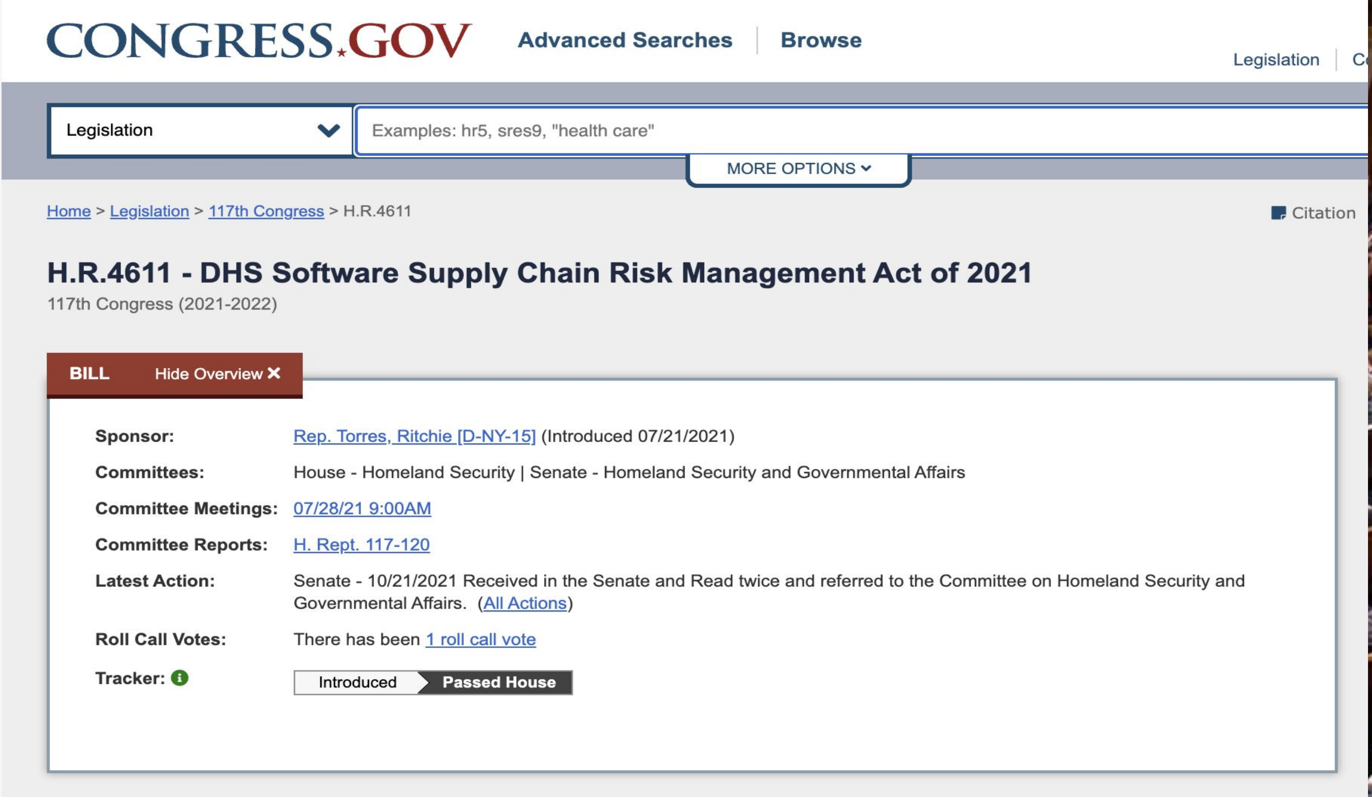
WHO USE SBOM AND FOR WHAT?

- For those who produce software, SBOMs are used to assist in the building and maintenance of their software, including upstream components.
- For those who choose or purchase software, SBOMs are used to inform pre-purchase assurance, negotiate discounts, or plan implementation strategies.
- For those who operate software, SBOMs are used to inform vulnerability management and asset management, to manage licensing and compliance, and to quickly identify software or component dependencies and supply chain risks.

JFrog

DevSecOps Day EMEA Unlock 2024

PASSED BY CONGRESS IN OCT 2021



Home > Legislation > 117th Congress > H.R.4611

H.R.4611 - DHS Software Supply Chain Risk Management Act of 2021

117th Congress (2021-2022)

Sponsor:	Rep. Torres, Ritchie [D-NY-15] (Introduced 07/21/2021)
Committees:	House - Homeland Security | Senate - Homeland Security and Governmental Affairs
Committee Meetings:	07/28/21 9:00AM
Committee Reports:	H. Rept. 117-120
Latest Action:	Senate - 10/21/2021 Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (All Actions)
Roll Call Votes:	There has been 1 roll call vote
Tracker:	Introduced > **Passed House**

THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

U.S. DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION
NTIA

Started discussion in 2018

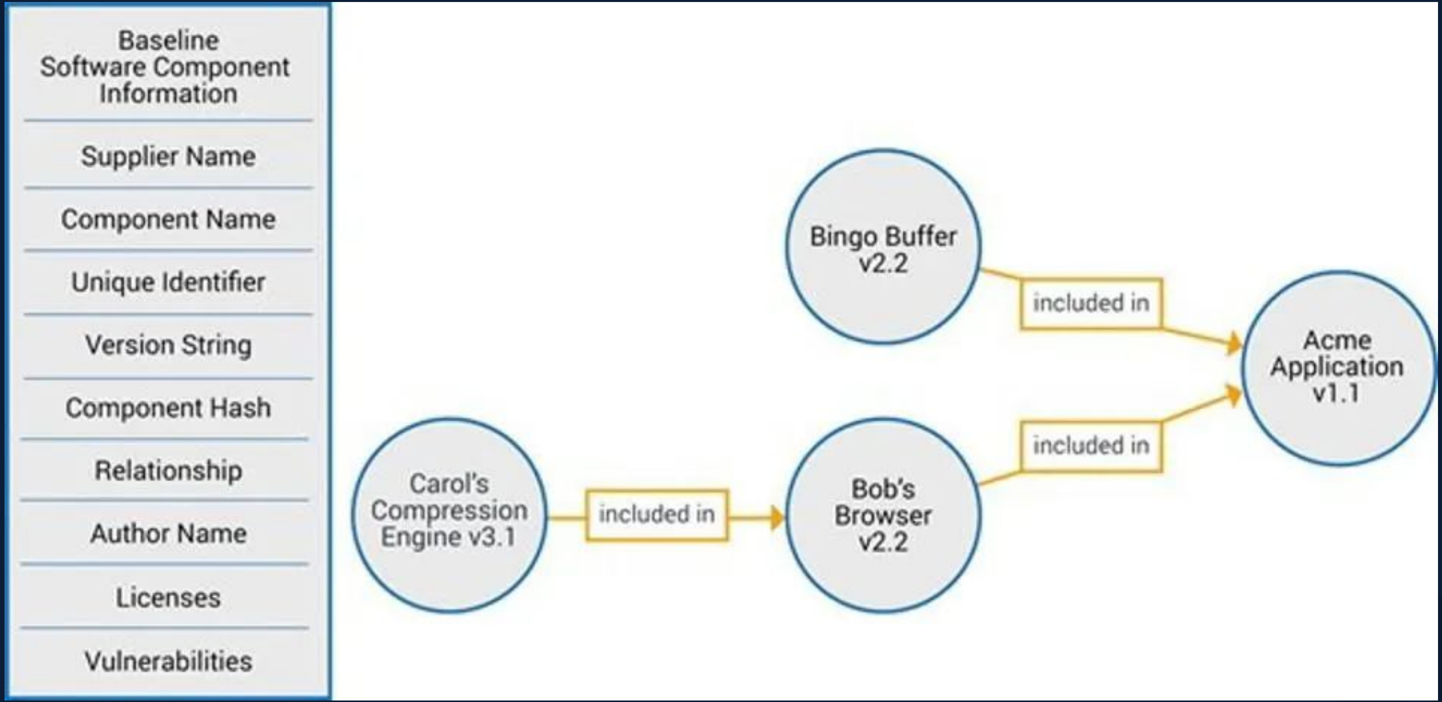
The Software Transparency Project

For Medical Device Manufacturers

A common method for safety guidelines with developing software

Inform Purchasers of devices of the software

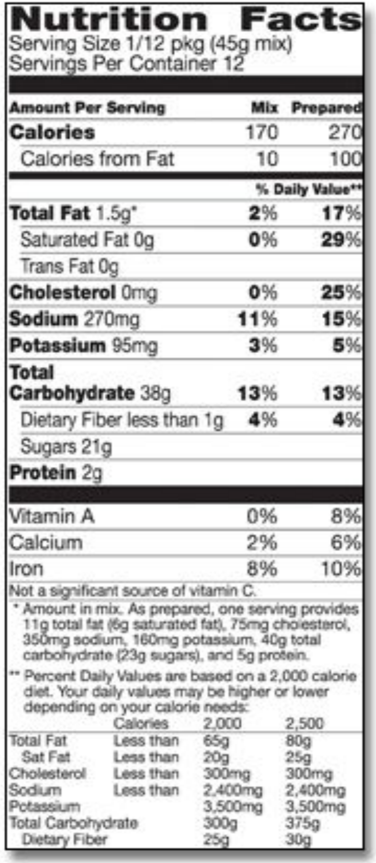
ACCORDING TO THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)



Baseline Software Component Information

- Supplier Name
- Component Name
- Unique Identifier
- Version String
- Component Hash
- Relationship
- Author Name
- Licenses
- Vulnerabilities

NO PRESERVATIVES - NO ARTIFICIAL FLAVORS - NO ARTIFICIAL COLORS
Betty Crocker
Betty's
ORIGINAL RECIPE
SCRATCH CAKE MIX
GERMAN CHOCOLATE DELIGHT
Just 7 INGREDIENTS IN THE BOX!



Nutrition Facts

Serving Size 1/12 pkg (45g mix)
Servings Per Container 12

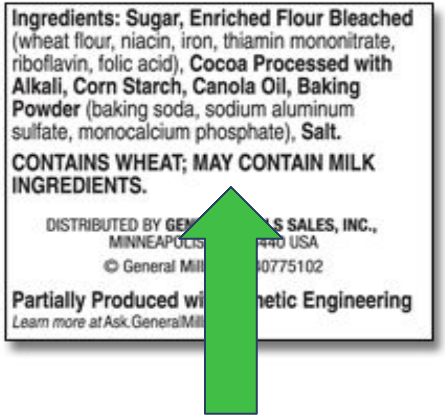
Amount Per Serving	Mix	Prepared
Calories	170	270
Calories from Fat	10	100
		% Daily Value**
Total Fat 1.5g*	2%	17%
Saturated Fat 0g	0%	29%
Trans Fat 0g		
Cholesterol 0mg	0%	25%
Sodium 270mg	11%	15%
Potassium 95mg	3%	5%
Total Carbohydrate 38g	13%	13%
Dietary Fiber less than 1g	4%	4%
Sugars 21g		
Protein 2g		
Vitamin A	0%	8%
Calcium	2%	6%
Iron	8%	10%

Not a significant source of vitamin C.

* Amount in mix. As prepared, one serving provides 11g total fat (6g saturated fat), 75mg cholesterol, 350mg sodium, 160mg potassium, 40g total carbohydrate (23g sugars), and 5g protein.

** Percent Daily Values are based on a 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs:

	Calories	2,000	2,500
Total Fat	Less than	65g	80g
Sat Fat	Less than	20g	25g
Cholesterol	Less than	300mg	300mg
Sodium	Less than	2,400mg	2,400mg
Potassium		3,500mg	3,500mg
Total Carbohydrate		300g	375g
Dietary Fiber		25g	30g



Ingredients: Sugar, Enriched Flour Bleached (wheat flour, niacin, iron, thiamin mononitrate, riboflavin, folic acid), **Cocoa Processed with Alkali, Corn Starch, Canola Oil, Baking Powder** (baking soda, sodium aluminum sulfate, monocalcium phosphate), **Salt.**

CONTAINS WHEAT; MAY CONTAIN MILK INGREDIENTS.

DISTRIBUTED BY GEN S SALES, INC.,
MINNEAPOLIS 440 USA
© General Mill 0775102

Partially Produced wi netic Engineering
Learn more at Ask.GeneralMill

INGREDIENTS

- 2 cups all-purpose flour
- 1 1/2 teaspoons baking soda
- 2 cups sugar
- 3/4 cup unsweetened cocoa powder
- 1 teaspoon salt
- 1 cup milk or buttermilk, almond, or coconut milk
- 1/2 cup melted coconut oil
- 2 large eggs
- 2 teaspoons vanilla extract
- 1 cup boiling water

LET’S TALK ABOUT CAKE INSTEAD…

LET’S LOOK AT OUR LOVELY CAKE AGAIN..

It might be part of a larger cake or just a cake

We know someone made

We know they mixed it somehow

It was baked in an oven

It will probably be decorated or maybe not

It might be tasty..

But we should probably taste it

We know they used ingredients

LET'S LOOK AT THE INGREDIENTS.. AND MORE

- 2 cups all-purpose flour
- 1 1/2 teaspoons baking soda
- 2 cups sugar
- 3/4 cup unsweetened cocoa powder
- 1 teaspoon salt
- 1 cup milk or buttermilk, almond, or coconut milk
- 1/2 cup melted coconut oil
- 2 large eggs
- 2 teaspoons vanilla extract
- 1 cup boiling water

1. Preheat the oven to 350 degrees F. Coat two 9-inch-round cake pans with cooking spray and line the bottoms with parchment paper.
2. Whisk the cocoa powder and 1 1/2 cups boiling water in a medium bowl until smooth; set aside. Whisk the flour, sugar, baking powder, baking soda and salt in a large bowl until combined. Add the eggs, vegetable oil, sour cream and vanilla and beat with a mixer on medium speed until smooth, about 1 minute. Reduce the mixer speed to low; beat in the cocoa mixture in a steady stream until just combined, then finish mixing with a rubber spatula. (The batter will be thin.)
3. Divide the batter between the prepared pans and tap the pans against the counter to help the batter settle. Bake until a toothpick inserted into the middle comes out clean, 30 to 40 minutes.

WHAT IF AN INGREDIENT CHANGED?

- 2 cups all-purpose flour
- 1 1/2 teaspoons baking soda
- 2 cups sugar
- 3/4 cup unsweetened cocoa powder
- 1 teaspoon salt
- 1 cup milk or buttermilk, almond, or coconut milk
- 1/2 cup melted coconut oil
- 2 large eggs
- 2 teaspoons vanilla extract
- 1 cup boiling water

1. Preheat the oven to 350 degrees F. Coat two 9-inch-round cake pans with cooking spray and line the bottoms with parchment paper.
2. Whisk the cocoa powder and 1 1/2 cups boiling water in a medium bowl until smooth; set aside. Whisk the flour, sugar, baking powder, baking soda and salt in a large bowl until combined. Add the eggs, vegetable oil, sour cream and vanilla and beat with a mixer on medium speed until smooth, about 1 minute. Reduce the mixer speed to low; beat in the cocoa mixture in a steady stream until just combined, then finish mixing with a rubber spatula. (The batter will be thin.)
3. Divide the batter between the prepared pans and tap the pans against the counter to help the batter settle. Bake until a toothpick inserted into the middle comes out clean, 30 to 40 minutes.

BAKING POWDER VS BAKING SODA

- 2 cups all-purpose flour
- 1 1/2 teaspoons baking soda
- 2 cups sugar
- 3/4 cup unsweetened cocoa powder
- 1 teaspoon salt
- 1 cup milk or buttermilk, almond, or coconut milk
- 1/2 cup melted coconut oil
- 2 large eggs
- 2 teaspoons vanilla extract
- 1 cup boiling water

1. Preheat the oven to 350 degrees F. Coat two 9-inch-round cake pans with cooking spray and line the bottoms with parchment paper.
2. Whisk the cocoa powder and 1 1/2 cups boiling water in a medium bowl until smooth; set aside. Whisk the flour, sugar, baking powder, baking soda and salt in a large bowl until combined. Add the eggs, vegetable oil, sour cream and vanilla and beat with a mixer on medium speed until smooth, about 1 minute. Reduce the mixer speed to low; beat in the cocoa mixture in a steady stream until just combined, then finish mixing with a rubber spatula. (The batter will be thin.)
3. Divide the batter between the prepared pans and tap the pans against the counter to help the batter settle. Bake until a toothpick inserted into the middle comes out clean, 30 to 40 minutes.

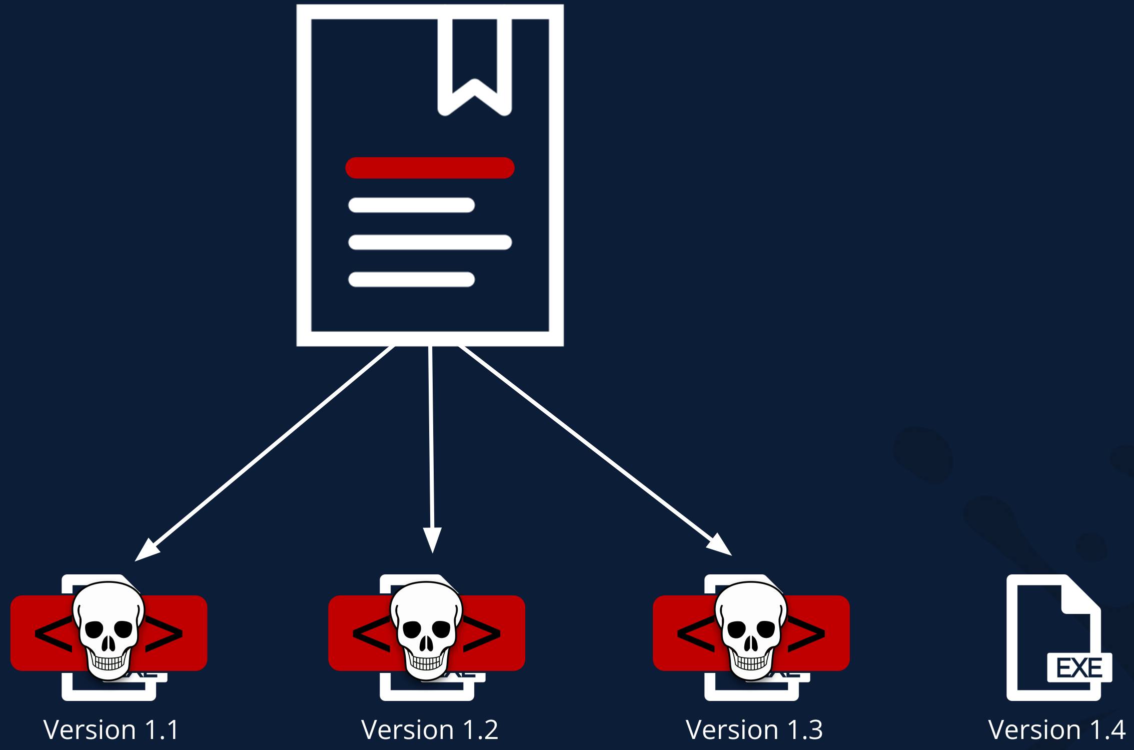
DOUBLE ACTING
BAKING POWDER
NET WT 8.1 OZ (230g)
Pure
Baking Soda
America's #1 Trusted Baking Soda Brand
Hundreds of uses like:
Fresh Box for Baking
NET WT. 1 LB. (454g)

BAKING SODA
BAKING POWDER

WHAT IS A SOFTWARE BILL OF MATERIALS?

- A list of ingredients that makes up what’s inside of software
- Including libraries and modules, can be open source or proprietary, free or paid, and the data can be widely available or access-restricted.
- Additionally, tooling, environmental information, settings, versions, etc.

SOFTWARE BILL OF MATERIAL



WHAT ABOUT A CAKE WITH LOTS OF LAYERS?

Each component of the cake is different

Each one has different ingredients

Each one was made different

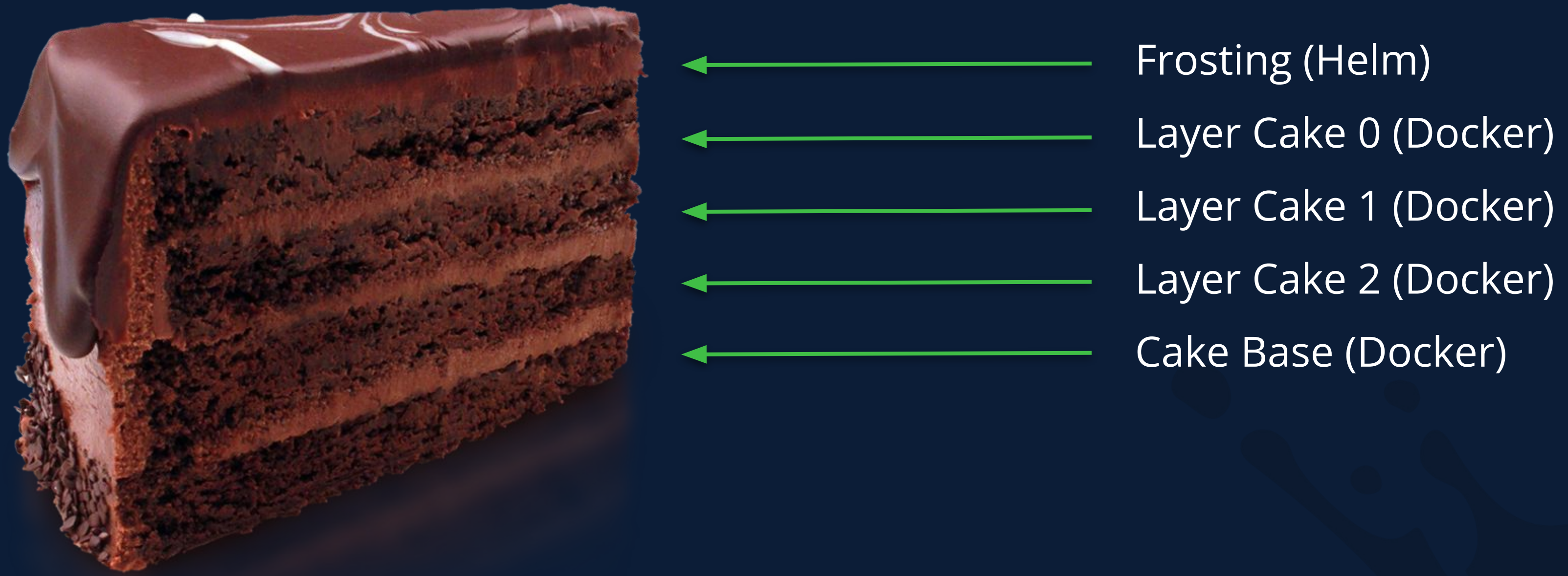
Each component could be made by someone else

Together is it is delicious

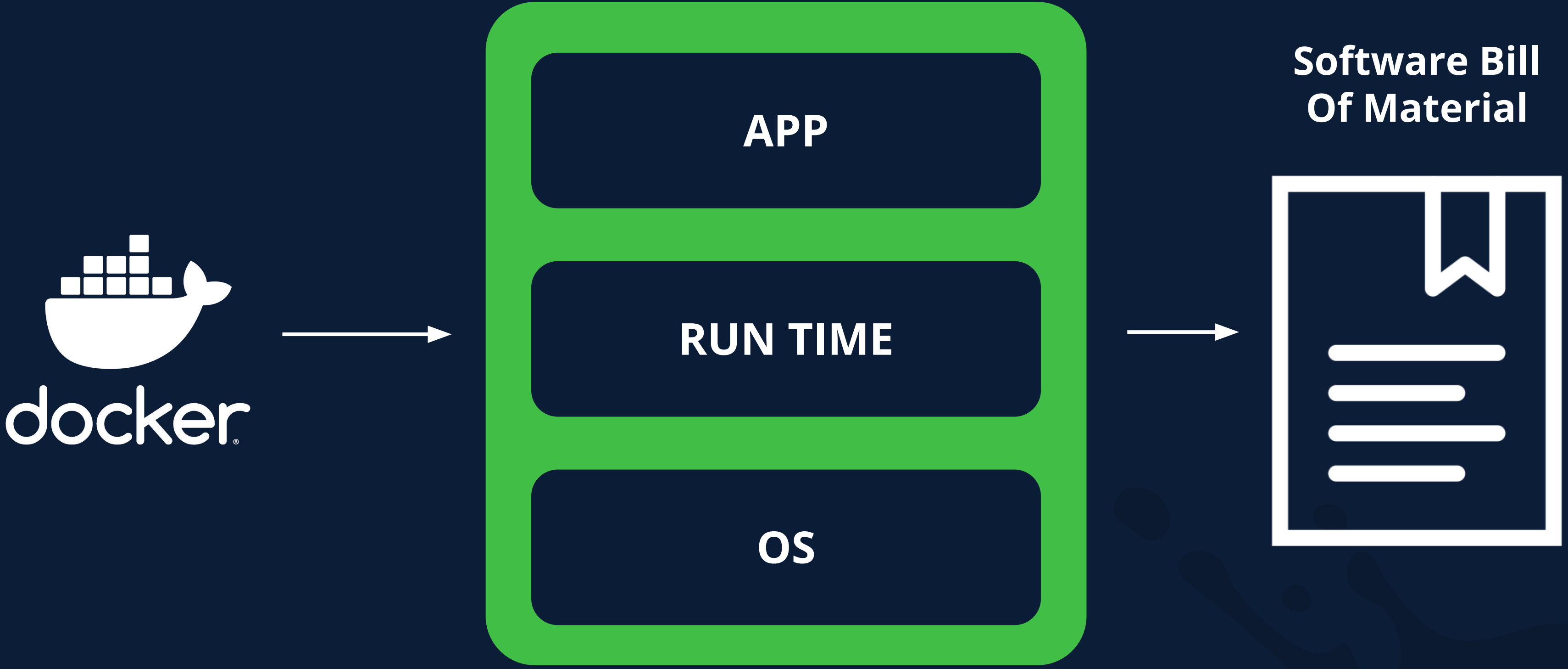
There might be different delivery locations

It might have a different purpose depending on location

WEB SERVICES LAYER CAKE



Each layer is a separate component that makes a whole web services



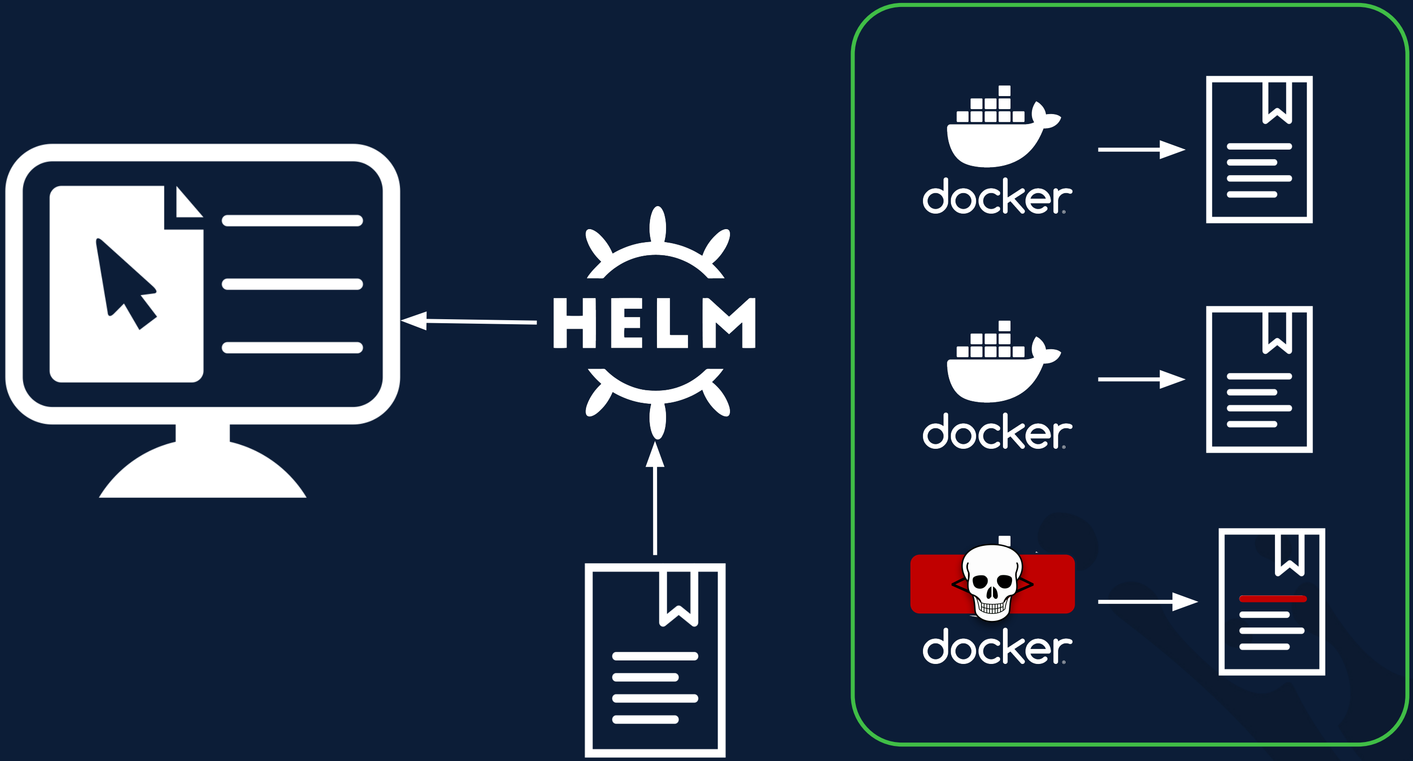
docker

APP

RUN TIME

OS

Software Bill Of Material


HELM
docker
docker
docker

WHO USE SBOM AND FOR WHAT?

- For those who produce software, SBOMs are used to assist in the building and maintenance of their software, including upstream components.
- For those who choose or purchase software, SBOMs are used to inform pre-purchase assurance, negotiate discounts, or plan implementation strategies.
- For those who operate software, SBOMs are used to inform vulnerability management and asset management, to manage licensing and compliance, and to quickly identify software or component dependencies and supply chain risks.

WHAT ARE THE BENEFITS OF SBOM?

- Identifying, mitigate, and avoiding known vulnerabilities(including patching and compensating controls for new vulnerabilities)
- Quantifying and managing licenses
- Identifying both security and license compliance requirements
- Enabling quantification of the risks inherent in a software package
- Comprehensive information on what environment and what setting were used
- Lower operating costs due to improved efficiencies and reduced unplanned and unscheduled work.

SPDX (SOFTWARE PACKAGE DATA EXCHANGE) VS CYCLONEDX

SPDX

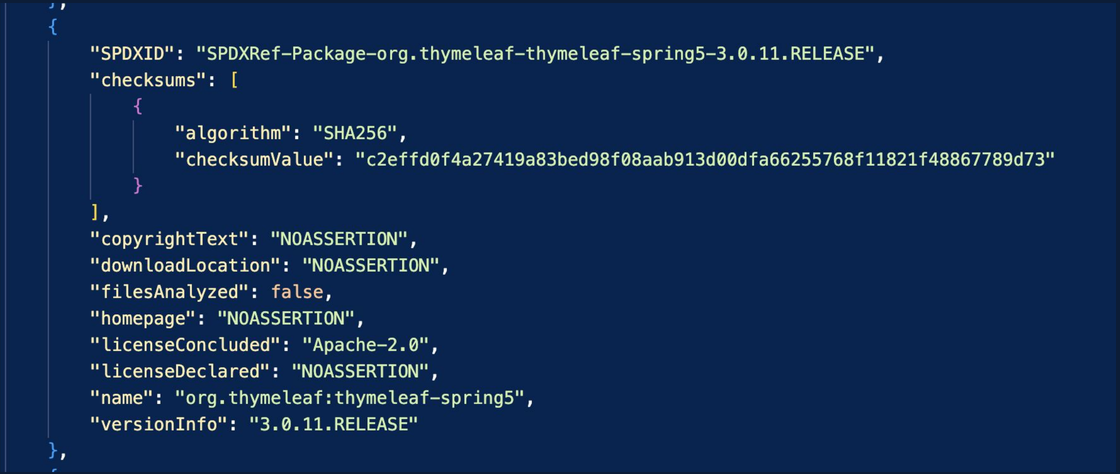
- Created back in 2011 as a license management tool
- Primarily designed as a way to manage open-source software licenses and share information about the packages.
- Format more useful for software development purposes

CycloneDX

- Newer format
- Allows users to create SBOMs (Software Bill of Materials) that provide detailed information about Software Components.
- More efficient vulnerability management tool as it details all the standard components of a software product.

REQUIRED FIELDS FOR SBOM

- Supplier Name
- Component Name
- Version of the Component.
- Other Unique Identifiers.
- Dependency Relationship.
- Author of SBOM Data.
- Timestamp.



```
},
{
    "SPDXID": "SPDXRef-Package-org.thymeleaf-thymeleaf-spring5-3.0.11.RELEASE",
    "checksums": [
        {
            "algorithm": "SHA256",
            "checksumValue": "c2effd0f4a27419a83bed98f08aab913d00dfa66255768f11821f48867789d73"
        }
    ],
    "copyrightText": "NOASSERTION",
    "downloadLocation": "NOASSERTION",
    "filesAnalyzed": false,
    "homepage": "NOASSERTION",
    "licenseConcluded": "Apache-2.0",
    "licenseDeclared": "NOASSERTION",
    "name": "org.thymeleaf:thymeleaf-spring5",
    "versionInfo": "3.0.11.RELEASE"
},
{
```

SBOM MISCONCEPTIONS

- Won’t SBOMs be a “roadmap to the attacker”?
- Does an SBOM require source code disclosure?
- Does a list of the software components I include expose my intellectual property?

DEMO

Oh yeah.. It’s time

JFrog

THANK YOU

DevSecOps Day EMEA Unlock 2024