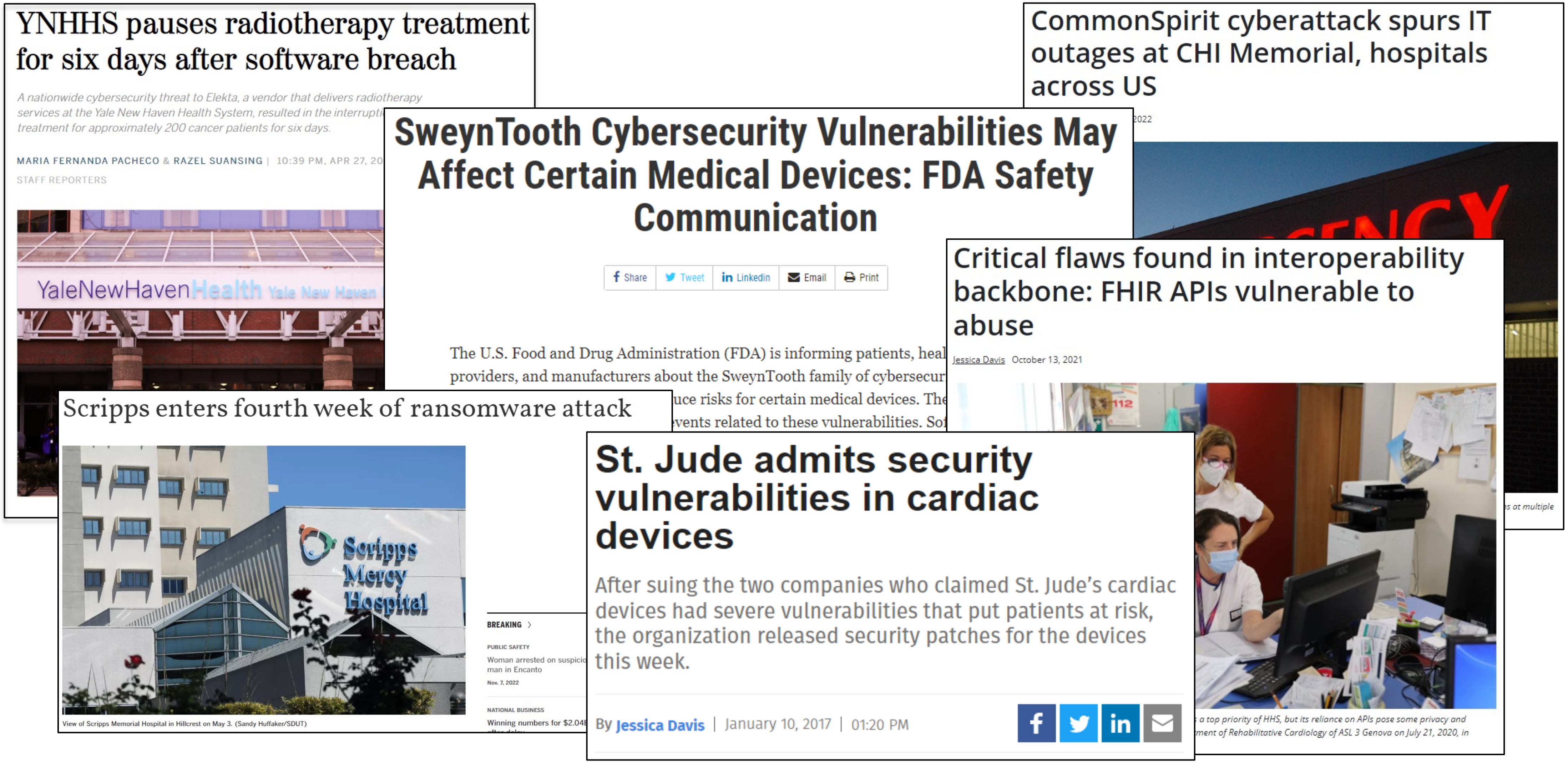
U.S. FOOD & DRUG ADMINISTRATION

FDA’s Medical Device Cybersecurity Program and SBOM

Jessica Wilkerson
Senior Cyber Policy Advisor and Medical Device Cybersecurity Team Lead
Office of Strategic Partnerships and Technology Innovation
Center for Devices and Radiological Health (CDRH)
Food and Drug Administration
jessica.wilkerson@fda.hhs.gov

CYBERSECURITY AND THE HEALTHCARE SECTOR

Cyber Incidents are Disrupting the Healthcare Sector's Ability to Deliver Quality Care



YNHHS pauses radiotherapy treatment for six days after software breach

A nationwide cybersecurity threat to Elekta, a vendor that delivers radiotherapy services at the Yale New Haven Health System, resulted in the interrupti treatment for approximately 200 cancer patients for six days.

MARIA FERNANDA PACHECO & RAZEL SUANSING | 10:39 PM, APR 27, 20

STAFF REPORTERS

CommonSpirit cyberattack spurs IT outages at CHI Memorial, hospitals across US

2022

s at multiple

SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication

Share | Tweet | Linkedin | Email | Print

The U.S. Food and Drug Administration (FDA) is informing patients, heal providers, and manufacturers about the SweynTooth family of cybersecur uce risks for certain medical devices. The events related to these vulnerabilities. Sof

Critical flaws found in interoperability backbone: FHIR APIs vulnerable to abuse

Jessica Davis October 13, 2021

a top priority of HHS, but its reliance on APIs pose some privacy and ment of Rehabilitative Cardiology of ASL 3 Genova on July 21, 2020, in

Scripps enters fourth week of ransomware attack

View of Scripps Memorial Hospital in Hillcrest on May 3. (Sandy Huffaker/SDUT)

BREAKING >

PUBLIC SAFETY

Woman arrested on suspicio man in Encanto

Nov. 7, 2022

NATIONAL BUSINESS

Winning numbers for $2.04B after delay

St. Jude admits security vulnerabilities in cardiac devices

After suing the two companies who claimed St. Jude's cardiac devices had severe vulnerabilities that put patients at risk, the organization released security patches for the devices this week.

By Jessica Davis | January 10, 2017 | 01:20 PM

Why does FDA CDRH Care about Medical Device Cybersecurity?

- Cybersecurity is patient safety – if you do not have a cybersecure device, you do not have a safe device
- Recent cyber incidents affecting medical devices and MDMs have created patient safety risks:
  - April 2021 ransomware incident at MDM delayed radiation therapy treatment availability by days to multiple weeks at ~40 hospitals across the country
  - February 2023 – 3 MDM ransomware incidents within 2 weeks, each of which could have (but did not) risk manufacturing capabilities, and therefore device availability
  - Ransomware and cyber incidents at hospitals continue to grow in frequency and severity, each of which represents a potential risk to device functionality at the affected institutions, and therefore care availability and patient safety
- Evaluating device cybersecurity as part of its safety and effectiveness has long been part of FDA’s process, and recent additional authorities have strengthened position
  - And these new authorities include SBOM

FDA’s New Authorities – Background

- The Consolidated Appropriations Act for 2023 was signed into law December 29, 2022 and includes the Food and Drug Omnibus Reform Act (FDORA)
- FDORA authorized a number of new amendments to the Food, Drug, and Cosmetic Act
- Section 3305 – Ensuring cybersecurity of medical devices
- Section 524B(b)(3) – Provide an SBOM, including commercial, open-source, and off-the-shelf software components for “cyber devices”

SOFTWARE BILL OF MATERIALS (SBOM)

Why Software Bill of Materials (SBOM)?

- Medical devices today incorporate significant amounts of software, both proprietary and open-source
- All software can be a source of risk as vulnerabilities are discovered and the software itself ages and becomes unsupported
- It is therefore imperative that medical device software supply-chains are documented and shared with regulators, users, and other appropriate parties
- **Software Bill of Materials (SBOM) enables this capability**

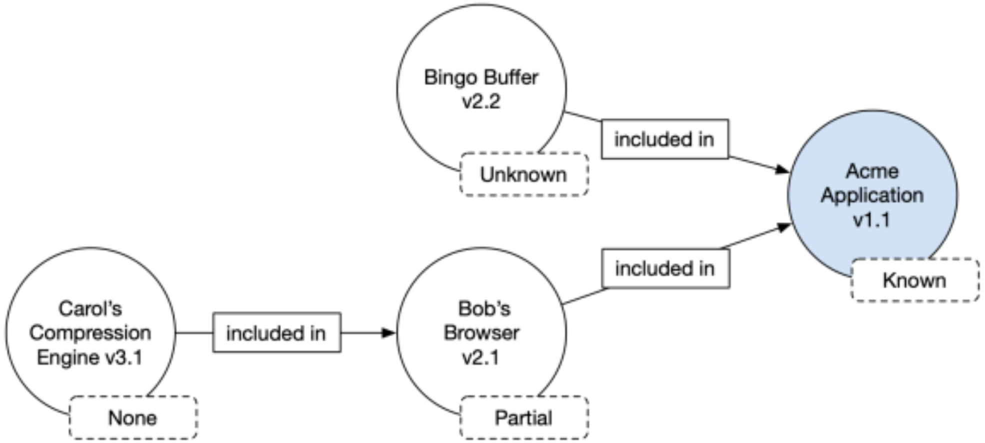
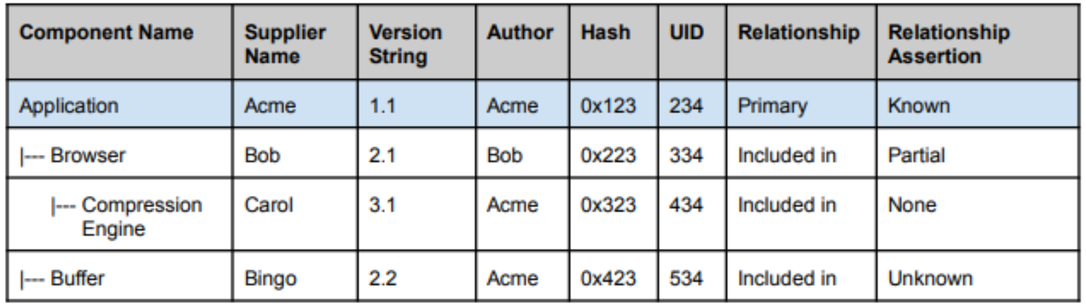


Figure 2: Conceptual SBOM graph with upstream relationship assertions



Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship	Relationship Assertion
Application	Acme	1.1	Acme	0x123	234	Primary	Known
|--- Browser	Bob	2.1	Bob	0x223	334	Included in	Partial
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in	None
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in	Unknown

Table 4: Conceptual SBOM table with upstream relationship assertions

Framing Phase 1 Update (ntia.gov)

FDA CDRH and SBOM

- New authorities require SBOMs for cyber devices
- FDA CDRH has also integrated SBOM into guidances related to medical device cybersecurity generally
- Recommendations are to:
  - Provide SBOMs to FDA to facilitate understanding/evaluation of device risk
  - Provide SBOMs to users to enable risk management activities
- Beyond "minimum" SBOM elements, FDA CDRH also wants:
  - Known vulnerability information
  - Support status
  - End of support/end of life dates

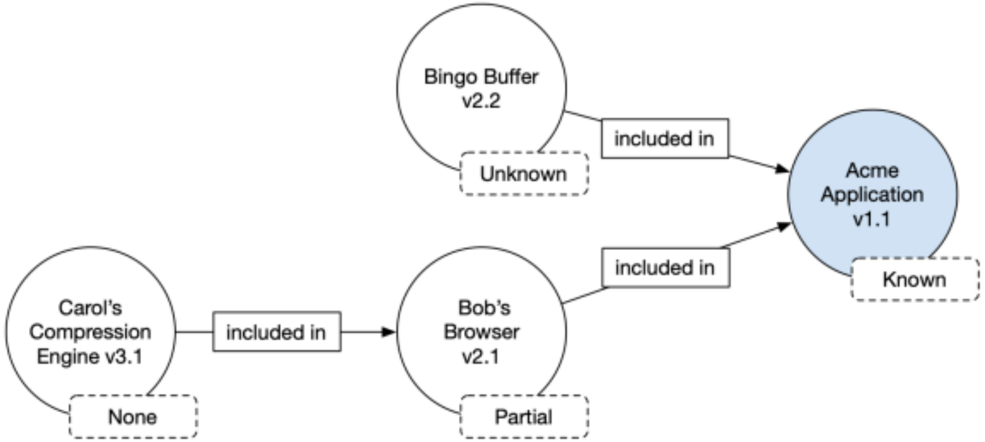
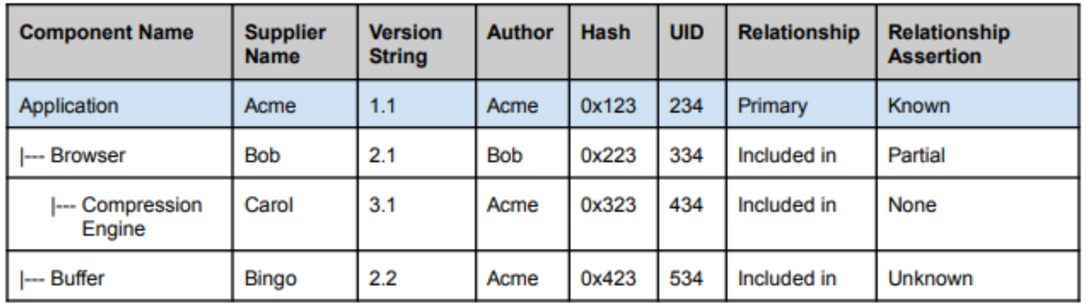


Figure 2: Conceptual SBOM graph with upstream relationship assertions



Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship	Relationship Assertion
Application	Acme	1.1	Acme	0x123	234	Primary	Known
|--- Browser	Bob	2.1	Bob	0x223	334	Included in	Partial
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in	None
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in	Unknown

Table 4: Conceptual SBOM table with upstream relationship assertions

Framing Phase 1 Update (ntia.gov)

IMDRF SBOM Overview

Purpose & Scope

- Provides a high-level description of an SBOM and best practices for the generation and use of an SBOM
  - Intended to provide greater detail on SBOM implementation for medical device stakeholders
- Scoped to the potential for patient harm

Key Components

- Provide recommendations for medical device manufacturers in SBOM generation, management, and distribution
- Provide recommendations to healthcare providers on ingestion and management of an SBOM
- Demonstrate SBOM use cases for risk management, vulnerability management, and incident response from the perspective of medical device manufacturers and healthcare providers

SBOM Use Cases

Premarket/Proactive Risk Management

- In reviews (FDA CDRH) and in acquisitions (private sector), extremely useful to know supply chain “risk” of devices approving or bringing into healthcare environment
  - Are there known(/exploited) vulnerabilities?
  - Is there unsupported software?
- SBOM allows FDA CDRH and private sector to evaluate these risks *before* the risks go “live”
- FDA resources: 2022 draft guidance
- Sector resources
  - IMDRF SBOM guidance
  - HSCC documents (Model Contracts, HIC-MaLTS, JSP, HICP, etc.)
  - NTIA/CISA SBOM documents

Postmarket/Reactive Risk Management

- Once devices are approved and in healthcare environments, new and emerging (or newly exploited) vulnerabilities may be discovered
  - And/or other incidents
- Time is of the essence to guard patient safety—need to quickly identify potentially impacted devices
- SBOM allows FDA CDRH and private sector to quickly search for potentially impacted devices and take action
- FDA resources: 2022 draft guidance
- Sector resources
  - IMDRF SBOM guidance
  - HSCC documents (Model Contracts, HIC-MaLTS, JSP, HICP, etc.)
  - NTIA/CISA SBOM documents

SBOM Use Cases – Others?

- Sector is at beginning of SBOM journey – as maturity improves, other use cases may arise
- FDA is excited to work with the sector to explore

CDRH Program Collaborations

FDA

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

IMDRF

Patient Communities

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

MDIC
MEDICAL DEVICE INNOVATION CONSORTIUM

Clinician Communities

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA
CYBER+INFRASTRUCTURE

MITRE

Security Researchers

International Standards

H-ISAC™
HEALTH - ISAC

SENSATO

MedISAO

QUESTIONS?

Thank you!

Jessica Wilkerson
Senior Cyber Policy Advisor and Medical Device Cybersecurity Team Lead
Office of Strategic Partnerships and Technology Innovation
Center for Devices and Radiological Health (CDRH)
Food and Drug Administration
jessica.wilkerson@fda.hhs.gov