


IAITAM ACE 2025

ITAM - Another Brick In The Wall

Effectively Secure Your Software Supply Chain With SBOM Management





1



Terry Divelbliss
Sr. VP, Marketing and Technical Alliances

- CSAM, CMAM, CAMSE, CITAD, CAIAM
- IAITAM Member #24
- Avid musician and car guy





April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

2

About Eracent

- ITAM, SAM and Cybersecurity solutions since 2000
- Headquarters in PA, R&D in Warsaw, global operations
- IT Management Center™ (ITMC)
- IT-Pedia® product enrichment data library
- Cybersecurity Management Suite™ (CSMS)



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

3

Software Supply Chain Under Threat

- Ongoing cyber incidents, breaches and hacks
- Current cybersecurity tools aren't stopping them
- Significant threat to the software supply chain
- Largely derived from open source software



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

4

Open Source Software Introduces Risk

- Open Source software is everywhere!

96%

of codebases



77%

of code within

70-90%

of all software

- Potential Vulnerabilities
- Obsolete Code
- License Risk





April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

5

Threat: Vulnerabilities

- Legacy vulnerability management tools monitor at the product and application level
- They didn't prevent high-profile hacks:
 - Log4j exploit
 - Solar Winds supply chain attack (2020)
 - XZ Utils Backdoor Incident (April 2024)





April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

6

Why? An Analogy...

- Designed and constructed a building
- Gated complex
- State-of-the-art locks
- Alarm system and cameras
- Protection from external threats, but...
- Nobody checked that door under the basement stairs
- **Bad actors are already hiding in there.**






April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

7

Threat: Vulnerabilities

- Components and Libraries can have vulnerabilities
- Behind the scenes, but critical
- Origin point of many hacks and exploits
- Tracked by NIST, GitHub Advisory, OSV, and other trusted organizations




April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

8

Threat: Obsolete Code

- Very old libraries and code are still used
- May be undermanaged or completely unmanaged
- Can be targeted by hackers




April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

9

Threat: License Type Risks

- License Types dictate how code may be utilized
- Wide range of restrictions and consequences
 - Permissive licenses
 - Strong Copyleft licenses
- Legal and financial ramifications
- AppDev teams: Choose wisely!



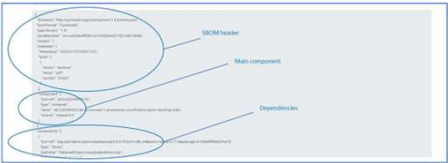
Eracent


April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

10

The Software Bill of Materials (SBOM)

- Provides an "ingredients list" of all components and libraries that comprise an application
- Shows the origin of each line of code






Eracent

April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

11

SBOM Management

- SBOMs are not new
- App Dev teams use for spot checks
- Use by end-user organizations for security *is* newer
- Embraced by CISA and other global standards organizations
- Different requirements for managing and analyzing contents
 - Software creators
 - Software consumers




Eracent

April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

12

Leveraging SBOM Content

- Vulnerability data from NIST NVD, GitHub Advisory, OSV, and other trusted sources
 - Risk scores, levels of criticality, dependencies, and more
- Mitigation and exemptions
- Alerts when new vulnerabilities are reported
- Version tracking and obsolescence management
- Visibility into license types for each component and library
- Associations with applications and installations



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

16

Libraries Summary and Details

Package Name	Version	Age	Dependencies	Label/Status	License	CVSS	MIT	SQL	JS	TS	PHP	License Type	Maint	Releas	Ver
libstdc++	4.8.5	10 years	libstdc++-dev	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libgcc	4.8.5	10 years	libgcc-sf	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libgomp	4.8.5	10 years	libgomp	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libquadmath	4.8.5	10 years	libquadmath	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libatomic	4.8.5	10 years	libatomic	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libitm	4.8.5	10 years	libitm	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libubsan	4.8.5	10 years	libubsan	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libssp	4.8.5	10 years	libssp	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libstdc++	4.8.5	10 years	libstdc++	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libgcc	4.8.5	10 years	libgcc	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libgomp	4.8.5	10 years	libgomp	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libquadmath	4.8.5	10 years	libquadmath	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libatomic	4.8.5	10 years	libatomic	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libitm	4.8.5	10 years	libitm	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libubsan	4.8.5	10 years	libubsan	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0
libssp	4.8.5	10 years	libssp	OK	Public Domain	0.0	0	0	0	0	0	Public Domain	0	0	0



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

17

Vulnerability Details and CVEs

Package Name	Library Name	Library Version	Age	Source	CVSS	MIT	SQL	JS	TS	PHP	License	Maint	Releas	Ver
libstdc++	libstdc++	4.8.5	10 years	libstdc++	0.0	0	0	0	0	0	Public Domain	0	0	0
libgcc	libgcc	4.8.5	10 years	libgcc	0.0	0	0	0	0	0	Public Domain	0	0	0
libgomp	libgomp	4.8.5	10 years	libgomp	0.0	0	0	0	0	0	Public Domain	0	0	0
libquadmath	libquadmath	4.8.5	10 years	libquadmath	0.0	0	0	0	0	0	Public Domain	0	0	0
libatomic	libatomic	4.8.5	10 years	libatomic	0.0	0	0	0	0	0	Public Domain	0	0	0
libitm	libitm	4.8.5	10 years	libitm	0.0	0	0	0	0	0	Public Domain	0	0	0
libubsan	libubsan	4.8.5	10 years	libubsan	0.0	0	0	0	0	0	Public Domain	0	0	0
libssp	libssp	4.8.5	10 years	libssp	0.0	0	0	0	0	0	Public Domain	0	0	0



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

18

License Type Details

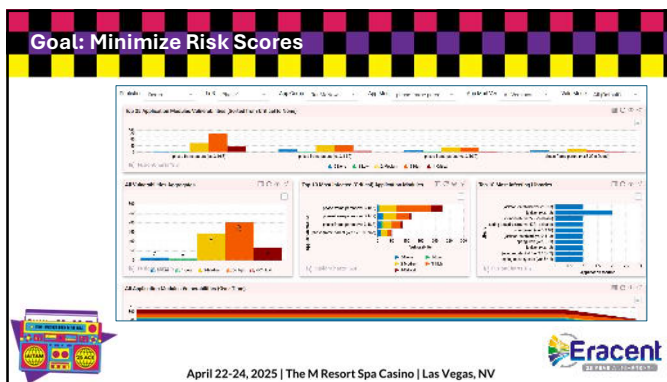
Lib	App Comp	Application Module	Version	Group Name	VCCount (for dep.)	Worst Lic. Cat. (dep.)	HScore
Phase1	RunMehow	phase frame-model-common	3.16.1	com.warrowsbanking	204	Copyright	2.0
Phase1	RunMehow	starlink60	6.3.20	com.warrowsbanking	204	Copyright	2.0
Phase1	RunMehow	starlink60	6.4.12	com.warrowsbanking	204	Copyright	2.0
Phase1	RunMehow	phase frame-parent	3.16.2	com.warrowsbanking	204	Copyright	2.0
Phase1	RunMehow	phase frame-parent	3.14.2	com.warrowsbanking	204	Copyright	2.0
Phase1	RunMehow	phase frame-parent	3.10.3	com.warrowsbanking	204	Copyright	2.0

Lib	Version	Age	Obso. error	Latest Version	Latest Age	EP-SB	CV	C	I	M	L	T	License Type	Mod	Int
libcrypto	1.0.1	1 year	Not Obsolete	2.1.1	2 days	0.00	0	0	0	0	0	0	Apache 2.0	1	1
libssl	1.0.1	1 year	Not Obsolete	2.1.1	2 days	0.00	0	0	0	0	0	0	Apache 2.0	1	1
libcrypto	1.0.1	1 year	Not Obsolete	2.1.1	2 days	0.00	0	0	0	0	0	0	Apache 2.0	1	1
libcrypto	1.0.1	1 year	Not Obsolete	2.1.1	2 days	0.00	0	0	0	0	0	0	Apache 2.0	1	1
libcrypto	1.0.1	1 year	Not Obsolete	2.1.1	2 days	0.00	0	0	0	0	0	0	Apache 2.0	1	1

Eracent

April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

19



20

Vulnerability Score Mitigation

Proposed Mitigated Score	CVE-2022-22965
Current Score	9.8
Proposed Score	5.0
Decision Required	Yes


Eracent

April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

21

Who Should Be Using SBOMs

- Risk Management (vulnerabilities, obsolescence and license risk)
- AppDev (vulnerabilities, obsolescence and license risk)
- Cybersecurity (vulnerabilities and obsolescence)
- ITAM and SAM (gatekeepers)
- Procurement (gatekeepers)
 - Request SBOMs!
 - Review during the sourcing/PoC process



Eracent

April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

22

Benefits

- Improve visibility and proactive planning
- Identify and mitigate behind-the-scenes threats
- Minimize incident response time
- Increase software supply chain security




Eracent

April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

23

Summary

- Mandate compliance is driving urgency and adoption
 - Government, Financial, Healthcare, Defense
 - Utilities and Critical Infrastructure
- Other industries are likely to follow as benefits are realized and publicized



Eracent

April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

24

Questions?



Thank You!




April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

25


Connect with Me!





terryd@eracent.com

linkedin.com/in/terry-divelbliss-581969/



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV

26
