BOMvault

SBOM Evidence Pack — SAMPLE

Acme Widget Service

Release v2.3.0 • Build 456 • Commit 9f8c1d2

Generated: 2025-08-19 | Generator: BomVault (demo)

• Purpose: reviewer-friendly summary + cryptographic materials for verification

• Contents: CycloneDX 1.6 (XML), SPDX 3.0 (JSON), VEX (JSON), in-toto provenance (JSONL), signature bundle, checksums

• Note: synthetic data for demonstration; links below are mock placeholders

BOMvault

Table of Contents

Mock links (not live):

• Verify page: https://verify.bomvault.example/EVP-20250819-001

• Artifact registry: https://registry.bomvault.example/org/acme/widget/releases/v2.3.0

• Verification docs: https://docs.bomvault.example/verify

BOMvault

Document Control & Change Log

Owner	Security Engineering
Approver	Head of Product Security
Doc ID	EVP-20250819-001
Version	1.1
Generated (UTC)	2025-08-19T10:32:00Z
Classification	External — SAMPLE
Signer (planned)	cosign (sigstore), AWS KMS key: arn:aws:kms:us-east-1:123456789012:key/abcd-****
Retention Policy	S3 Object Lock (configurable 7-year retention)

Revision History

Rev	Date (UTC)	Change	By
1.1	2025-08-19T10:32:00Z	Improved text wrapping; retention note updated	Security Eng / BomVault
1.0	2025-08-19T10:00:00Z	Initial sample evidence pack	Security Eng / BomVault

BOMvault

1. Executive Summary

Project	Acme Widget Service
Version	v2.3.0
Build / Commit	456 / 9f8c1d2
SBOM Stats	187 components (36 direct, 151 transitive); 7 u licenses
Vulnerability Summary	Critical: 0 | High: 2 | Medium: 5 | Low: 12
Key Outcome	0 criticals. 2 highs mitigated (1 fixed, 1 not_affe VEX).

This pack summarizes SBOM artifacts and verification materials. Machine-readable files are referenced with SHA-256 hashes. Signature bundle and in-toto provenance enable cryptographic verification of integrity and origin.

2. Artifact Inventory & Hashes

- acme-widget-v2.3.0-sbom.spdx.json — 691 bytes

  `SHA-256: 494bc69d606eadda0ffd698187f2a903c0bf879c689b5a431071775ad45b932a`

- acme-widget-v2.3.0-sbom.cyclonedx.xml — 907 bytes

  `SHA-256: 8d9fbb8f14009bd768004e1b2879c7614ed9ac3ffd5a01d24810384ad314f200`

- acme-widget-v2.3.0-vex.json — 1157 bytes

  `SHA-256: 18f4313c855d145fb550412c7fc3c85b342f7007ed52be95ebbc053b15091f97`

- acme-widget-v2.3.0-provenance.intoto.jsonl — 935 bytes

  `SHA-256: bf2e3b3f3dbf639713b3105eb7ab5d8db373351c75e8d35b984739fc1c9304b1`

- acme-widget-v2.3.0-signature.cosign.bundle — 45 bytes

  `SHA-256: b9a176056e19d6f6ef54bbf0604506ba131ca5aca48323186018302b4a33f901`

All artifacts are included in the downloadable pack. This PDF is a human-readable summary.

Mock registry: https://registry.bomvault.example/org/acme/widget/releases/v2.3.0

3. Verification Guide

Verify checksums:

```
shasum -a 256 acme-widget-v2.3.0-sbom.spdx.json acme-widget-v2.3.0-sbom.cyclonedx.xml \   acme-widg
acme-widget-v2.3.0-provenance.intoto.jsonl \   acme-widget-v2.3.0-signature.cosign.bundle
```

Compare outputs to the SHA-256 values listed in Section 2 and checksums.txt.

Verify signature bundle:

```
cosign verify-blob --bundle acme-widget-v2.3.0-signature.cosign.bundle \   acme-widget-v2.3.0-sbom.
```

Expect a valid signature and matching digest.

Verify in-toto provenance:

(1) Parse acme-widget-v2.3.0-provenance.intoto.jsonl and locate 'subject' digests.

(2) Confirm each subject sha256 matches the artifact’s computed checksum.

Mock verify page: https://verify.bomvault.example/EVP-20250819-001 (not live)

4. SBOM Diff Summary (vs v2.2.5)

Added:

- urllib3 2.2.1
- pyyaml 6.0.1
- click 8.1.7

Updated:

- openssl 3.0.0 → 3.0.2
- flask 2.3.3 → 3.0.0
- requests 2.31.0 → 2.32.2
- jinja2 3.1.2 → 3.1.4

Removed:

- deprecated-lib 0.9.1
- old-parser 1.2.0

BOMvault

5. VEX Summary

CVE	Component	Severity	VEX State	Justification/Remediation
CVE-2024-12345	openssl 3.0.2	High	fixed	Upgraded to 3.0.2
CVE-2023-45678	libyaml 0.2.5	High	not_affected	Build-only; vulnerable code not present

Residual risk: no critical vulnerabilities; high items addressed via fix or VEX justification.

BOMvault

6. Compliance Mapping

Control / Expectation	Status	Notes
CISA Minimum SBOM Elements present	Pass	All required fields present
CycloneDX 1.6 + SPDX 3.0 included	Pass	Both formats provided
VEX linked to SBOM items	Pass	CycloneDX VEX 1.5
in-toto/SLSA provenance	Pass	Subjects reference SBOM files
Signature bundle (cosign)	Pass	Bundle attached for artifacts
Immutable storage (WORM)	Pass	S3 Object Lock (configurable 7-year retention)

Decl. storage policy: immutable evidence artifacts retained under WORM policy. This sample pack is illustrative; links are non-functional.

Appendices — Artifacts & Policies (Index)

Appendix A: SBOM (CycloneDX 1.6 XML) — acme-widget-v2.3.0-sbom.cyclonedx.xml

Appendix B: SBOM (SPDX 3.0 JSON) — acme-widget-v2.3.0-sbom.spdx.json

Appendix C: VEX (CycloneDX 1.5 JSON) — acme-widget-v2.3.0-vex.json

Appendix D: in-toto/SLSA provenance (JSONL) — acme-widget-v2.3.0-provenance.intoto.jsonl

Appendix E: Signature bundle (cosign) — acme-widget-v2.3.0-signature.cosign.bundle

Appendix F: Policies — Immutability & Retention statement (WORM 7 years)

Artifact registry (mock): https://registry.bomvault.example/org/acme/widget/releases/v2.3.0

Verification docs (mock): https://docs.bomvault.example/verify

Note: This PDF is view-only; sample data for demonstration.