Module 7 Lab 1

Secure Software Supply Chain with Software Bill of Materials (SBOMs)

Part 1: SBOM Generation

SPDX SBOM:

```
/workspaces/class-ENG298-mod7-lab1/ng911-dev main ❯ syft . -o spdx-json > ../deliverables/sbom_syft_spdx.json                    08:20:56 PM
 ✔ Indexed file system                                                                                                            .
 ✔ Cataloged contents                                                                   cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21329efb0336fc02a82e1839a8
   ├── ✔ Packages                        [107 packages]
   ├── ✔ File digests                    [3 files]
   ├── ✔ File metadata                   [3 locations]
   └── ✔ Executables                     [0 executables]
[0000]  WARN no explicit name and version provided for directory source, deriving artifact ID from the given path (which is not ideal)
A newer version of syft is available for download: 1.38.0 (installed version is 1.37.0)
```

CycloneDX SBOM:

```
/workspaces/class-ENG298-mod7-lab1/ng911-dev main ❯ trivy fs . --format cyclonedx --output ../deliverables/sbom_trivy_cdx.json                    08:24:53 PM
2025-12-06T20:25:30-05:00       INFO    "--format cyclonedx" disables security scanning. Specify "--scanners vuln" explicitly if you want to include vulnerabilities in
the "cyclonedx" report.
2025-12-06T20:25:30-05:00       INFO    [python] Licenses acquired from one or more METADATA files may be subject to additional terms. Use `--debug` flag to see all aff
ected packages.
2025-12-06T20:25:30-05:00       INFO    [npm] To collect the license information of packages, "npm install" needs to be performed beforehand    dir="test_suite/test_fil
es/_old/TPLan_Config/VS_Code/node_modules"
2025-12-06T20:25:30-05:00       INFO    Number of language-specific files       num=2

📣 Notices:
  - Version 0.68.1 of Trivy is now available, current version is 0.67.2

To suppress version checks, run Trivy scans with the --skip-version-check flag
```

Calculating the number of components reported by Trivy in the CycloneDX SBOM:

```
/workspaces/class-ENG298-mod7-lab1/ng911-dev main ❯ cat ../deliverables/sbom_trivy_cdx.json | jq '.components | length'
106
```

As shown above, Syft reported 107 components and Trivy reported 106 components.

One major difference between the SPDX and CycloneDX SBOMs is in how they're organized. For example, CycloneDX groups files ("applications") and packages ("libraries") together in one list, called "components." However, SPDX separates these into two lists, called "packages" and "files."

Part 2: SBOM Vulnerability Analysis

Grype Analysis:

```
/workspaces/class-ENG298-mod7-lab1/ng911-dev main ❯ grype sbom:../deliverables/sbom_syft_spdx.json -o table > ../deliverables/vuln_analysis_grype.txt
 ✔ Scanned for vulnerabilities     [11 vulnerability matches]
   ├── by severity: 0 critical, 4 high, 6 medium, 1 low, 0 negligible
A newer version of grype is available for download: 0.104.1 (installed version is 0.103.0)
```

Grype Analysis Results:

deliverables > vuln_analysis_grype.txt

```
NAME          INSTALLED  FIXED IN  TYPE    VULNERABILITY        SEVERITY  EPSS           RISK
cryptography  43.0.0     44.0.1    python  GHSA-79v4-65xg-pq4g  Low       1.1% (77th)    0.3
fonttools     4.57.0     4.60.2    python  GHSA-768j-98cg-p3fv  Medium    0.2% (36th)    < 0.1
setuptools    72.1.0     78.1.1    python  GHSA-5rjg-fvgr-3xxf  High      < 0.1% (25th)  < 0.1
requests      2.32.3     2.32.4    python  GHSA-9hjg-9r4m-mvj7  Medium    < 0.1% (25th)  < 0.1
brotli        1.1.0      1.2.0     python  GHSA-2qfp-q593-8484  High      < 0.1% (4th)   < 0.1
urllib3       2.2.2      2.5.0     python  GHSA-pq67-6m6q-mj2v  Medium    < 0.1% (2nd)   < 0.1
urllib3       2.2.2      2.5.0     python  GHSA-48p4-8xcf-vxj5  Medium    < 0.1% (0th)   < 0.1
urllib3       2.2.2      2.6.0     python  GHSA-2xpw-w6gg-jr37  High      N/A            N/A
urllib3       2.2.2      2.6.0     python  GHSA-gm62-xv2j-4w53  High      N/A            N/A
cryptography  43.0.0     43.0.1    python  GHSA-h4gh-qq45-vh27  Medium    N/A            N/A
scapy         2.5.0                python  GHSA-cq46-m9x9-j8w2  Medium    N/A            N/A
```

First 5 Vulnerabilities:

Component	Version	CVE	Severity	Comment
cryptography	43.0.0	CVE-2024-12797	Low	Vulnerable OpenSSL included in cryptography wheels
fonttools	4.57.0	CVE-2025-66034	Medium	fontTools is Vulnerable to Arbitrary File Write and XML injection in fontTools.varLib
setuptools	72.1.0	CVE-2025-47273	High	setuptools has a path traversal vulnerability in PackageIndex.download that leads to Arbitrary File Write
requests	2.32.3	CVE-2024-47081	Medium	Requests vulnerable to .netrc credentials leak via malicious URLs
brotli	1.1.0	CVE-2025-6176	High	Scrapy is vulnerable to a denial of service (DoS) attack due to flaws in brotli decompression implementation

For example, the setuptools vulnerability, found here in the NVD database, allows an attacker to use setuptools to write to any file that the setuptools program has access to, effectively bypassing all user input validation enforced by the setuptools program.

Part 3: Deliverables

Reflecting on this lab, one thing that struck me was the heavy reliance on the CVE database for the entire process. If a vulnerability is never reported to this database, it seems as if the vulnerability will never get caught when using such SBOM analysis tools. This is scary, particularly if a malicious actor were to take control of the CVE database (or the maintainers of the CVE database voluntarily decided not to publish a specific vulnerability).