

REPO URL: <https://github.com/Brendan-H/eng298-fa25-mod7-sbom-lab1>

```
@Brendan-H → /workspaces/eng298-fa25-mod7-sbom-lab1 (main) $ git clone https://github.com/tamu-edu/ng911-dev.git
Cloning into 'ng911-dev'...
remote: Enumerating objects: 2357, done.
remote: Counting objects: 100% (1555/1555), done.
remote: Compressing objects: 100% (852/852), done.
remote: Total 2357 (delta 859), reused 1321 (delta 688), pack-reused 802 (from 4)
Receiving objects: 100% (2357/2357), 8.62 MiB | 27.68 MiB/s, done.
Resolving deltas: 100% (1165/1165), done.
@Brendan-H → /workspaces/eng298-fa25-mod7-sbom-lab1 (main) $ cd ng911-dev
@Brendan-H → /workspaces/eng298-fa25-mod7-sbom-lab1/ng911-dev (main) $ syft -o spdx-json > ../deliverables/sbom_syft_spdx.json
✓ Indexed file system
✓ Cataloged contents
├── 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)
@Brendan-H → /workspaces/eng298-fa25-mod7-sbom-lab1/ng911-dev (main) $ trivy fs --format cyclonedx --output ../deliverables/sbom_trivy_cdx.json
2025-11-26T01:16:37Z INFO "--format cyclonedx" disables security scanning. Specify "--scanners vuln" explicitly if you want to include vulnerabilities in the "cyclonedx" report.
2025-11-26T01:16:37Z INFO [python] Licenses acquired from one or more METADATA files may be subject to additional terms. Use "--debug" flag to see all affected packages.
2025-11-26T01:16:37Z INFO [npm] To collect the license information of packages, "npm install" needs to be performed beforehand dir="test_suite/test_files/_old/TPlan_Config/V5_Code/nod
e_modules"
2025-11-26T01:16:37Z INFO Number of language-specific files num=2
@Brendan-H → /workspaces/eng298-fa25-mod7-sbom-lab1/ng911-dev (main) $ ls ../deliverables/
README.md sbom_syft_spdx.json sbom_trivy_cdx.json

@Brendan-H → /workspaces/eng298-fa25-mod7-sbom-lab1 (main) $ cd ../ng911-dev/
@Brendan-H → /workspaces/eng298-fa25-mod7-sbom-lab1/ng911-dev (main) $ gype sbom:../deliverables/sbom_syft_spdx.json -o table > ../deliverables/vuln_analysis_gype.txt
✓ Vulnerability DB [updated]
✓ Scanned for vulnerabilities [8 vulnerability matches]
├── by severity: 0 critical, 2 high, 5 medium, 1 low, 0 negligible
@Brendan-H → /workspaces/eng298-fa25-mod7-sbom-lab1/ng911-dev (main) $ head -20 ../deliverables/vuln_analysis_gype.txt
NAME INSTALLED FIXED IN TYPE VULNERABILITY SEVERITY EPSS RISK
cryptography 43.0.0 44.0.1 python GHSA-79v4-65xg-pq4g Low 1.0% (75th) 0.3
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-9h1g-9r4m-mvj7 Medium < 0.1% (20th) < 0.1
brotli 1.1.0 1.2.0 python GHSA-2qfp-q593-8484 High < 0.1% (3rd) < 0.1
urllib3 2.2.2 2.5.0 python GHSA-pq67-6m6q-mj2v Medium < 0.1% (1st) < 0.1
urllib3 2.2.2 2.5.0 python GHSA-48p4-8xcq-vxj5 Medium < 0.1% (0th) < 0.1
cryptography 43.0.0 44.0.1 python GHSA-h4gh-qg45-vh27 Medium N/A N/A
scapy 2.5.0 python GHSA-cq46-m9x9-j8w2 Medium N/A N/A
@Brendan-H → /workspaces/eng298-fa25-mod7-sbom-lab1/ng911-dev (main) $
```

Part 1

The Syft spdx SBOM references 107 packages and 215 relationships, whereas the Trivy cdx one only has 105 components and 106 dependencies. One major difference between the spdx and cdx SBOMs is that syft's sbom is separated into packages, files, and relationships, but the cdx has components, dependencies, and vulnerabilities.

Part 2

CVE	Severity	Component	Version	Comment
CVE-2024-12797	Low	cryptography	43.0.0	Vulnerable OpenSSL included in cryptography wheels
CVE-2025-47273	High	setuptools	72.1.0	setuptools has a path traversal vulnerability in PackageIndex.d ownload that leads to Arbitrary File Write
CVE-2024-47081	Medium	requests	2.32.3	Requests vulnerable to .netrc

				credentials leak via malicious URLs
CVE-2025-6176	High	brotli	1.1.0	Scrapy is vulnerable to a denial of service (DoS) attack due to flaws in brotli decompression implementation
CVE-2025-5018 1	Medium	urllib3	2.2.2	urllib3 redirects are not disabled when retries are disabled on PoolManager instantiation

I chose CVE-2025-47273. It is a high severity vulnerability because it could possibly lead to remote code execution because attackers can write to the filesystem so they can plant malicious code.

I was surprised that the nextgen911 repo had any vulnerabilities, much less high severity ones. The process was smooth, though I did find it odd that the gype output reports GHSA codes rather than CVEs. It seems like github is trying to reinvent the wheel with their own vulnerability database.