How I Learned to Stop Worrying and Love the SBOM

OVE Tagung, 6.10.2022 Vienna

LIMES SECURITY

Software Bill of Material

- “formal record containing the details and supply chain relationships of various components used in building software”
  (US legislation)

- “a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements
  (EU legislation)

A sample BOM is shown below:

Component	Version	Vulnerabilities - CVEs	Notes
jQuery	1.4.4	CVE-2011-4969	
libxml2	2.9.4	CVE-2016-5131	To be fixed

Providing a SBOM becomes an obligation

- Executive Order on Improving the Nation's Cybersecurity
  - Sec. 4. Enhancing Software Supply Chain Security
  - Such guidance shall include standards, procedures, or criteria regarding [...] providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website
- Draft of EU Cyber Security Act
  - „identify and document vulnerabilities and components contained in the
  - product, including by drawing up a software bill of materials in a commonly
  - used and machine-readable format covering at the very least the top-level
  - dependencies of the product“

and also helps to comply with IEC 62443-4-1

- SM-9: Security Requirements For Externally Provided Components
  - A process shall be employed to identify and manage the security risks of all externally provided components used within the product
  - receive and/or monitor notifications about security-related issues from the component supplier
  - It is recommended that there be an inventory of components from third party suppliers in order to facilitate defect management
- SM-6: File integrity
  - A process shall be employed to provide an integrity verification mechanism for all scripts, executables and other important files included in a product.

Challenges SBOMs help to resolve

- Transparency of third-party components, versioning, and known vulnerabilities
- Enables vulnerability and patch management
- Supports licensing compliance

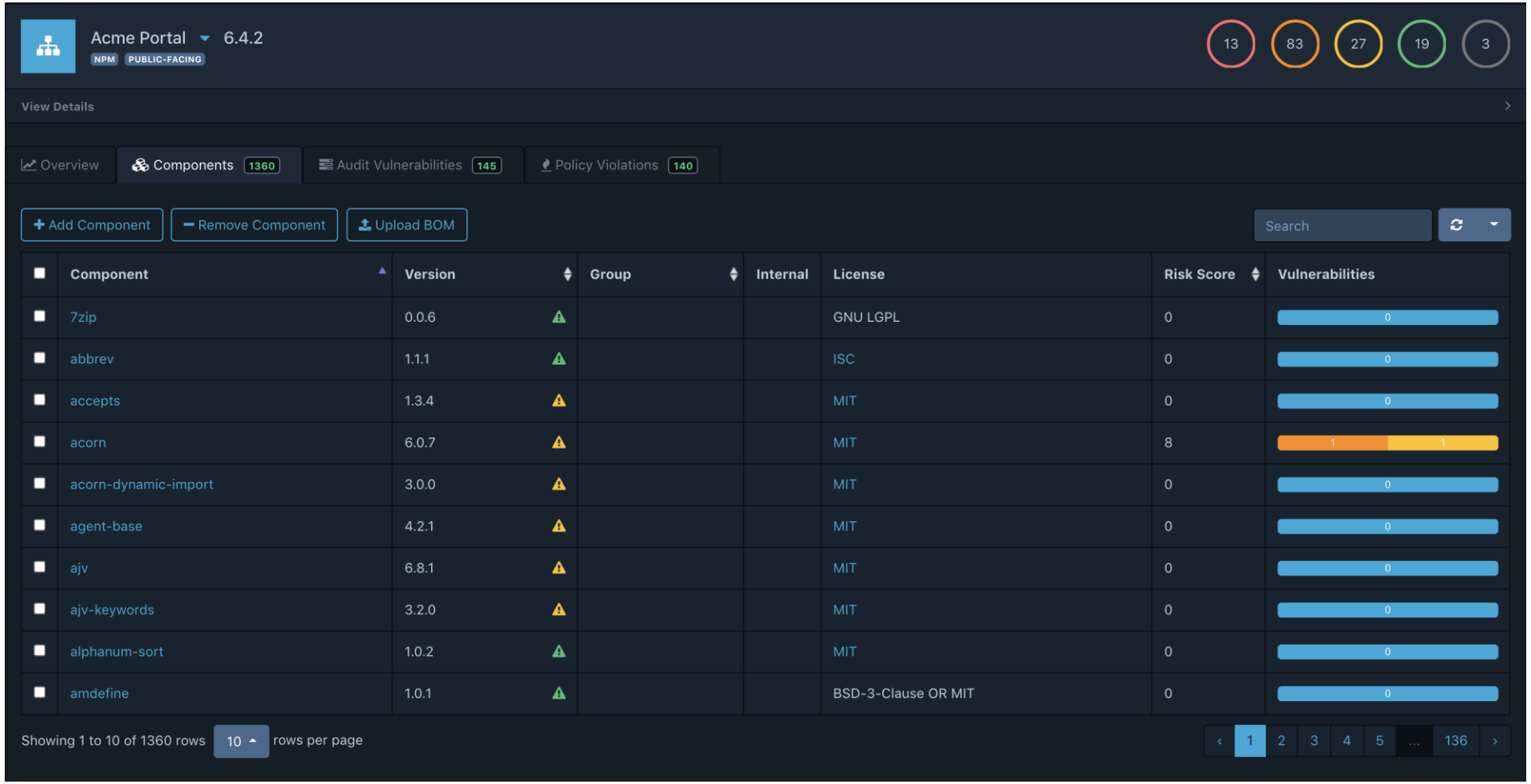
Example: Use Syft to create SBOM

- Syft
  - https://github.com/anchore/syft
  - CLI tool and Go library for generating a Software Bill of Materials (SBOM) from container images and filesystems
  - Able to create signed SBOM attestationst
  - Convert between SBOM formats, such as CycloneDX, SPDX, and Syft's own format
  - syft <image> -o <format>
  - syft nginx –i cyclonedx-json

Example: Use Dependency Track to work with SBOM

- OWASP Dependency Track
  - https://dependencytrack.org/
  - Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain
  - consumes and analyzes CycloneDX BOMsIdentify and remediate vulnerable components

Example: Use Dependency Track to work with SBOM

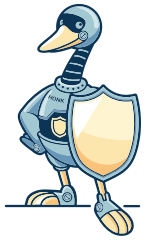


How to evaluate open source software?

- Unmitigated known vulnerabilities
- Security Documentation
- Active Community
- Evaluation Results
- Do our own security verification and validation testing?

Evaluating Open Source: Security Scorecards

- https://securityscorecards.dev/
- Part of the Open Source Security Foundation
- Security Scorecards assesses open source projects for security risks through a series of automated checks
- Security Scorecards can be used in a couple of different ways:
  - Run automatically on code you own **using the GitHub Action**
  - Run manually on your (or somebody else's) project **via the Command Line**
- Security Scorecards checks for vulnerabilities affecting different parts of the software supply chain including **source code**, **build**, **dependencies**, **testing**, and project **maintenance**.



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Evaluating Open Source: other options

- Coverity Scan
  - Free static code analysis for open source, public results
  - https://scan.coverity.com/projects
- Sonar Cloud
  - Free static code analysis for open source, public results
  - https://sonarcloud.io/explore/projects
- Collection of further resources:
  - https://owasp.org/www-community/Free_for_Open_Source_Application_Security_Tools

Other examples of how to make suppliers part of your processes

- Supplier qualification
  - Process to evaluate the supplier (not the deliverable)
  - Focus on processes and capabilities
  - e.g. certifications, questionnaire about secure development activities and quality management
- Security requirements for the deliverables
  - Technical requirements, e.g. two factor authentication, supported ciphers, …
  - Maintenance requirements, e.g. how long will security updates be available? For open source: is there an active community? Are there regular commits?
- Verification of deliverables
  - Test cases for deliverables
  - Can the suppliers do the tests themselves?

LIMES SECURITY

- Why we love the SBOM
  - Transparency in the supply chain
  - Security and OSS license managing
  - Evolving tooling
  - Regulations require it if we love it or not

LIMES
SECURITY

+43 720 510251

office@limessecurity.com