OWASP Dependency-Check

Chapter Meeting

OWASP_Geneva
2015/10/19

OWASP
The Open Web Application Security Project

About Me

- Thomas Hofer
- Java DEV / AppSec
- OWASP Geneva Board

- State of Geneva

- @thhofer
- thomas.hofer@owasp.org

Outline

- Context
- How it works / Integration
- Sample results
- False positives
- Links
- Q&A

Context

- OWASP Top 10 – 2013
  - A9 – Using components with known vulnerabilities
    - Prevalence: Widespread
    - Detectability: Difficult

- Dependency-Check project
  - Java & .Net
  - Team: Jeremy Long, Will Stranathan, Steve Springett

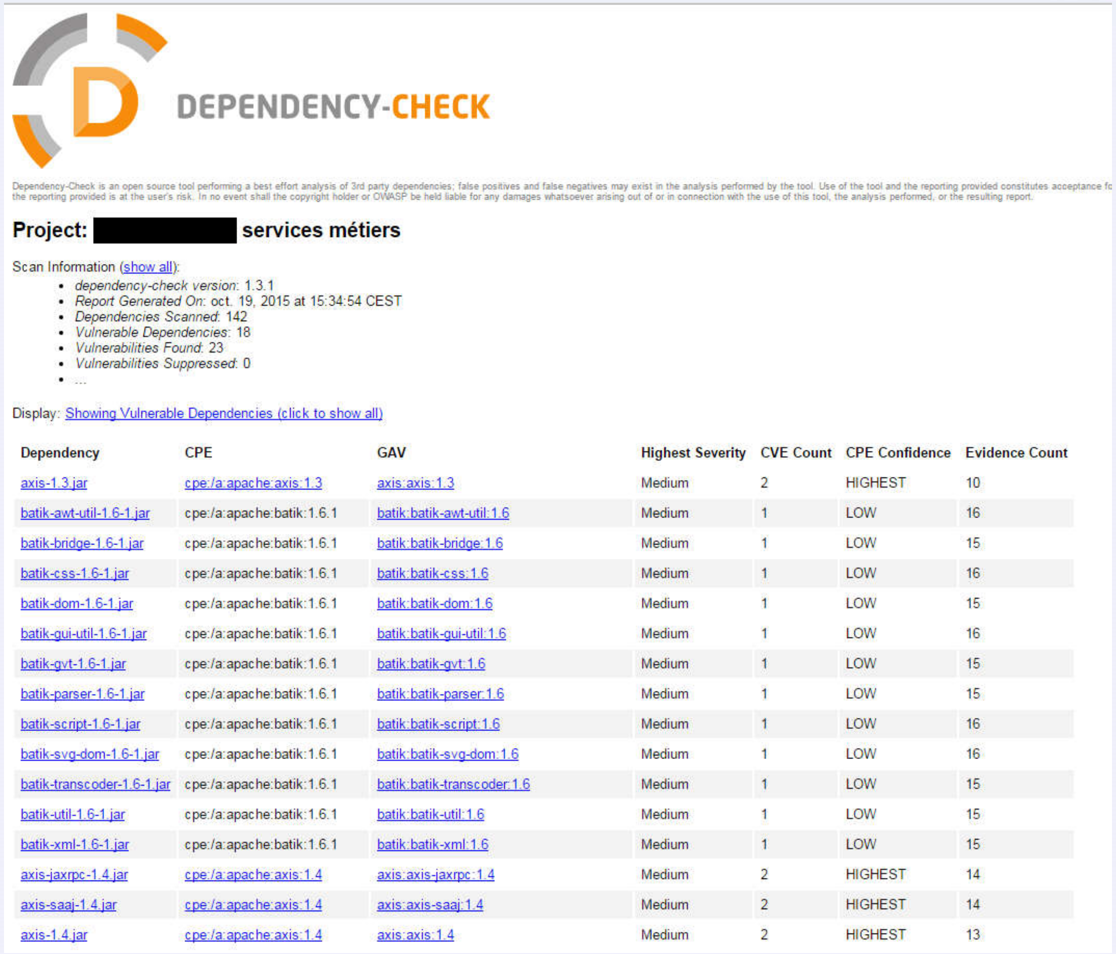
How it works

- Searches NVD CVE
  - Based on data extracted from libs compared to CPE identifiers

- Can run as
  - Maven plugin
  - Ant task
  - Gradle plugin
  - Jenkins plugin

Sample results

OWASP
The Open Web Application Security Project



Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance fo
the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

Project: [redacted] services métiers

Scan Information (show all):

- *dependency-check version*: 1.3.1
- *Report Generated On*: oct. 19, 2015 at 15:34:54 CEST
- *Dependencies Scanned*: 142
- *Vulnerable Dependencies*: 18
- *Vulnerabilities Found*: 23
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
axis-1.3.jar	cpe:/a:apache:axis:1.3	axis:axis:1.3	Medium	2	HIGHEST	10
batik-awt-util-1.6-1.jar	cpe:/a:apache:batik:1.6.1	batik:batik-awt-util:1.6	Medium	1	LOW	16
batik-bridge-1.6-1.jar	cpe:/a:apache:batik:1.6.1	batik:batik-bridge:1.6	Medium	1	LOW	15
batik-css-1.6-1.jar	cpe:/a:apache:batik:1.6.1	batik:batik-css:1.6	Medium	1	LOW	16
batik-dom-1.6-1.jar	cpe:/a:apache:batik:1.6.1	batik:batik-dom:1.6	Medium	1	LOW	15
batik-gui-util-1.6-1.jar	cpe:/a:apache:batik:1.6.1	batik:batik-gui-util:1.6	Medium	1	LOW	16
batik-gvt-1.6-1.jar	cpe:/a:apache:batik:1.6.1	batik:batik-gvt:1.6	Medium	1	LOW	15
batik-parser-1.6-1.jar	cpe:/a:apache:batik:1.6.1	batik:batik-parser:1.6	Medium	1	LOW	15
batik-script-1.6-1.jar	cpe:/a:apache:batik:1.6.1	batik:batik-script:1.6	Medium	1	LOW	16
batik-svg-dom-1.6-1.jar	cpe:/a:apache:batik:1.6.1	batik:batik-svg-dom:1.6	Medium	1	LOW	16
batik-transcoder-1.6-1.jar	cpe:/a:apache:batik:1.6.1	batik:batik-transcoder:1.6	Medium	1	LOW	15
batik-util-1.6-1.jar	cpe:/a:apache:batik:1.6.1	batik:batik-util:1.6	Medium	1	LOW	15
batik-xml-1.6-1.jar	cpe:/a:apache:batik:1.6.1	batik:batik-xml:1.6	Medium	1	LOW	15
axis-jaxrpc-1.4.jar	cpe:/a:apache:axis:1.4	axis:axis-jaxrpc:1.4	Medium	2	HIGHEST	14
axis-saaj-1.4.jar	cpe:/a:apache:axis:1.4	axis:axis-saaj:1.4	Medium	2	HIGHEST	14
axis-1.4.jar	cpe:/a:apache:axis:1.4	axis:axis:1.4	Medium	2	HIGHEST	13

False positives

- Suppression Filters – added in 1.0.7 (Dec 2013)
  - Simple way to remove false positives

```
<?xml version="1.0" encoding="UTF-8"?>
<suppressions
xmlns="https://www.owasp.org/index.php/OWASP_Dependency_Check_Suppression">
  <suppress>
    <notes><![CDATA[
    file name: spring-core-3.0.0.RELEASE.jar
    ]]></notes>
    <sha1>4F268922155FF53FB7B28AECA24FB28D5A439D95</sha1>
    <cpe>cpe:/a:vmware:springsource_spring_framework:3.0.0</cpe>
  </suppress>
</suppressions>
```

Links

OWASP
The Open Web Application Security Project

- Project page
  https://www.owasp.org/index.php/OWASP_Dependency_Check
- Documentation
  http://jeremylong.github.io/DependencyCheck/index.html
- Source
  https://github.com/jeremylong/DependencyCheck

- Jeremy's original presentation
  http://jeremylong.github.io/DependencyCheck/general/dependency-check.pdf

Q&A

Questions?