OWASP dependency check analysis na backendu ništagrama

Za proveru ranjivih paketa na backendu ništagrama korišćen je org.owasp.dependency-check-maven verzija 6.2.2.

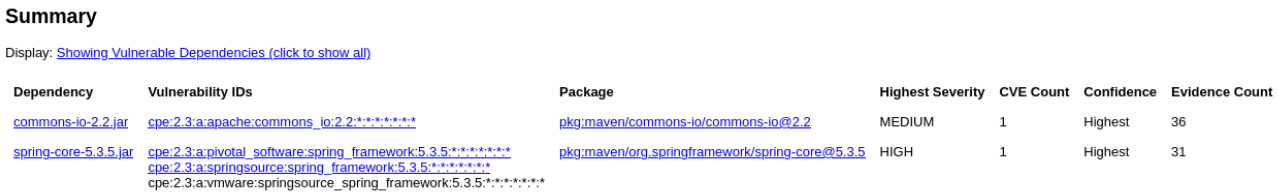
```
<plugin>
    <groupId>org.owasp</groupId>
    <artifactId>dependency-check-maven</artifactId>
    <version>6.2.2</version>
    <executions>
        <execution>
            <goals>
                <goal>check</goal>
            </goals>
        </execution>
    </executions>
</plugin>
```

Figure 1: Dependency-check-maven dodat kao plugin u jednom od maven projekata

Nakon pokretanja dependency checka na svakom od mikroservisa dobili smo izveštaje koji se nalaze na putanji nistagram-services/documentation/dependency-checks/{ime-mikroservisa}-dependency-check-report-before.html

Najčešći ranjivi paketi na koje smo naišli su: commons-io-2.4.jar, spring-core-5.3.6.jar.

Ranjivost paketa commons-io-2.4.jar smo ispravili tako što smo ga obnovili na verziju 2.8.0 a ranjivost paketa spring-core-5.3.6.jar tako što smo spring-boot obnovili na verziju 2.5.1 sa starije 2.4.5, dok smo ranjivost vezanu za hibernate-validator koja nam se javila nakon obnavljanja spring-boot-a na noviju verziju ispravili obnavljanjem istog na 7.0.1.Final.



Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
commons-io-2.2.jar	cpe:2.3:a:apache:commons_io:2.2:*:*:*:*:*:*:*	pkg:maven/commons-io/commons-io@2.2	MEDIUM	1	Highest	36
spring-core-5.3.5.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.5:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.5:*:*:*:*:*:*:* cpe:2.3:a:vmware:springsource_spring_framework:5.3.5:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@5.3.5	HIGH	1	Highest	31

Figure 2: Primer izveštaja dobijenog pokretanjem maven dependecy checka na jednom od mikroservisa

Svi izveštaje dobijeni nakon obnavljanja ranjivih paketa se mogu pronaći na putanji nistagram-services/documentation/dependency-checks/{ime-mikroservisa}-dependency-check-report-after.html