OWASP Dependency Check

Za utvrđivanje ranjivosti mikroservisa i gateway-a naše aplikacije korišćen je *Maven Dependency Check* verzije v6.2.1. Ranjivosti koje smo tom prilikom uvidjeli i otklonili su sljedeće:

Frontend ranjive komponente:

1. Prelazak na noviju verziju jQuery: v3.5.1, sve verzije jQuery-ja prije 3.4.0 su ranjive na rukovanje sa jQuery.extend(true, {}, ...).
2. Prelazak na noviju verziju Bootstrap: v4.1.3, sve verzije prije 4.1.2 mogu biti ranjive na XSS napade.

Auth service, publishing service ranjivi dependency:

1. batik-css-1.11.jar
2. commons-beanutils-1.9.3.jar
3. guava-19.0.jar (Guava predstavlja skup osnovnih i proširenih biblioteka koje uključuju klase utility klase, IO klase i Google-ove kolekcije. Sve verzije do v24.0.0 omogućuju napadačima da izvrše napad na našu aplikaciju. Ranjivost riješena prelaskom na verziju 30.1.1 koja nije ranjiva).
4. commons-io-2.6.jar
5. spring-core-5.3.6.jar (U Spring Framework-u verzije niže od v5.3.6 su ranjive na privilegovane radnje, tako na primjer zlonamjerni korisnik sa lokalnom autentifikacijom može čitati ili modifikovati datoteke kojim ne smije pristupati. Ranjivost riješena prelaskom na verziju 5.3.7 koja nije ranjiva)
6. log4j-slf4j-impl-2.11.2.jar, log4j-api-2.11.2.jar (Biblioteke koju smo koristili za kreiranje i održavanje log fajlova. Nakon otkrivanje ove ranjivosti smo se posvetili istraživanju prijetnje po naš sistem koji nosi ovaj dependency i preuzimanju rizika za datu prijetnju. Kako je ozbiljnost ranjivosti na veoma niskom nivou, uradili smo sve što je bilo u našoj moći da rizik svedemo na minimuim, naši log fajlovi su zaštićeni putem ACL, imamo dobru validaciju i na backendu i na frontendu i kako je vjerovatnoća za ovakav napad jako niska, odlučili smo se da živimo sa navedenom ranjivošću i da biblioteku ipak zadržimo).

Following service ranjivi dependency:

1. log4j-1.2.17.jar
2. batik-css-1.11.jar
3. commons-beanutils-1.9.3.jar
4. guava-19.0.jar (Ranjivost riješena prelaskom na verziju 30.1.1 koja nije ranjiva)
5. commons-io-2.6.jar
6. spring-core-5.3.6.jar (Ranjivost riješena prelaskom na verziju 5.3.7 koja nije ranjiva)
7. hibernate-validator-6.2.0.Final.jar (Hibernate Validator je biblioteka koja omogućava izraze za validaciju ulaznih podataka aplikacije, anotacije kao sto su npr. @NotNull, @NotEmpty itd. Niže verzije imaju ranjivost u interpolaciji poruka i omogućuju napadačima da zaobiđu ulazne kontrole i umetnu zlonamjerni kod. Ranjivost riješena prelaskom na najnoviju verziju 7.0.1Final)

Activity service, story service, media service ranjivi dependency:

1. log4j-1.2.17.jar
2. batik-css-1.11.jar
3. commons-beanutils-1.9.3.jar
4. guava-19.0.jar (Ranjivost riješena prelaskom na verziju 30.1.1 koja nije ranjiva)
5. commons-io-2.6.jar
6. hibernate-validator-6.2.0.Final.jar (Ranjivost riješena prelaskom na najnoviju verziju 7.0.1Final)

Zuul gateway ranjivi dependency:

1. batik-css-1.11.jar
2. commons-beanutils-1.9.3.jar
3. commons-io-2.6.jar
4. log4j-1.2.17.jar
5. xstream-1.4.14.jar

Sve ranjivosti su riješene preko suppressions.xml. To su sve bili lažno pozitivni rezultati. Zbog načina na koje provjerava dependency-je u okviru biblioteka Dependency Check može dati lažne pozitivne rezultate. Ove lažno pozitivne rezultate smo suzbili uz pomoć suppressions.xml fajla. Drugih ranjivosti u ovom servisu nije bilo.

PKI ranjivi dependency:

1. log4j-1.2.17.jar
2. batik-css-1.11.jar
3. commons-beanutils-1.9.3.jar
4. log4j-core-2.11.2.jar
5. commons-io-2.6.jar
8. spring-core-5.3.4.jar (Ranjivost riješena prelaskom na verziju 5.3.7 koja nije ranjiva)