**Bezbednosna analiza *third-party* komponenti**

Backend

* Za analizu Maven *dependency*-ja korišćenih u Agentskoj aplikaciji i u mikroservisima, upotrebili smo [OWASP Dependency-Check v5.3.2](https://owasp.org/www-project-dependency-check/). Na osnovu dobijenih izveštaja otklonili smo određene ranjivosti *update*-ovanjem verzije Spring-a sa v2.2.7 na v2.3.0., što je sa sobom povuklo i *update*-ovanje nekih od problematičnih *dependency*-ja.
* Izveštaji nakon *update*-ovanja verzije Spring-a: [Link](https://drive.google.com/drive/folders/1X_J89Ldj-VqaAkwXLPvI_-Wqws3-UJV7?usp=sharing)
* Iz priloženih izveštaja se mogu uočiti ranjivosti sledećih dependency-ja:
  1. dependency-check-core-5.3.2.jar: jquery-3.4.1.min.js *(Severity: medium)*

- Regularni izraz upotrebljen u funkciji [jQuery.htmlPrefilter](https://api.jquery.com/jQuery.htmlPrefilter/) uvodi ranjivost koja se može iskorititi za XSS napad. Ranjivost je posledica nedovoljno dobre sanitizacije ulaznih podataka. Napadač može da prosledi maliciozan kod aplikaciji koja se oslanja na pomenutu funkciju i tako izvrši proizvoljan JavaScript kod u korisnikovom browser-u.

- Uspešna zloupotreba ove ranjivosti može omogućiti napadaču da ukrade osetljive informacije, promeni izgled stranica, izvrši *phishing* i *drive-by-download* napade.

- Ranjivost je otklonjena već u narednoj verziji jQuery v3.5.0.

- Kako ovaj dependency nismo mi direktno uveli, već ga koristi OWASP Dependency-Check, nismo smeli da ga *update*-ujemo, jer prelazak na verziju v3.5.0 zahteva i izmene u kodu koje mi ne možemo sprovesti.

* 1. spring-cloud-netflix-eureka-server-2.2.2.RELEASE.jar: wro.js *(Severity: medium)*

- Ranjivosti zavedene u NIST-ovoj NVD bazi pod [CVE-2015-9251](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-9251) i [CVE-2019-11358](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-11358). Obe su posledica neažurne verzije jQuery biblioteke koju navedeni *dependency* koristi, a odnose se na ranjivost u vidu mogućeg XSS napada.

- Prema [CVE-2015-9251](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-9251), ranjivost je prisutna kod jQuery verzija pre v3.0.0 ako se *cross-domain* Ajax zahtevi sprovode bez postavljanja *dataType*-a. Konkretno, upotreba:   
 *$.get(url, function(...) { ... })*; (nesigurno)

umesto:

*$.ajax(url, { jsonp: false, dataType: 'json' }).done(function(...) { ... });* (sigurno)

prouzrokuje ranjivost, gde napadač može kao odgovor da vrati *text/javascript* sadržaj u vidu malicioznog koda koji će se izvršiti unutar *eval()* funkcije.

- Prema [CVE-2019-11358](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-11358), ranjivost je prisutna kod jQuery verzija pre v3.4.0, kod kojih *$.extend* funkcija može biti zloupotrebljena da se izvrši *prototype pollution* napad. To znači da je moguće da se proizvoljno modifikuju *property*-ji Object prototipa, a samim tim bi bili prisutni u svim objektima. Ovo se može potvrditi sledećim kodom:  
 *$.extend(true, {}, JSON.parse('{"\_\_proto\_\_": {"devMode": true}}'))*

*console.log({}.devMode); // rezultat -> true*

- Kao i u slučaju prethodnog *dependency*-ja, ovo nismo bili u mogućnosti da otklonimo *update*-ovanjem. Takođe, nismo ni sigurni da li su ranjive funkcije i upotrebljene u ovom *dependency*-ju.

* 1. spring-security-core-5.3.2.RELEASE.jar *(Severity: high),*  
     spring-security-rsa-1.0.9.RELEASE.ja *(Severity: high),*  
     spring-security-crypto-5.3.2.RELEASE.jar *(Severity: high)*

- Sva tri *dependency*-ja su u NIST-ovoj NVD bazi zavedena pod [CVE-2018-1258](https://nvd.nist.gov/vuln/detail/CVE-2018-1258), jer je i uzrok ranjivosti isti. Kada se Spring *framework*-a v5.0.5 koristi u kombinaciji sa bilo kojom verzijom Spring Security-ja, javlja se ranjivost vezana za autorizaciju. Napadač može iskoristiti tu ranjivost da, iako neautorizovan, dobije pristup resursima kojima bi pristup trebao biti zaštićen.

- Obzirom da mi koristimo Spring *framework* v5.3.2, pojava ove ranjivosti u izveštaju je bila nelogična. Istraživanjem ([link](https://github.com/jeremylong/DependencyCheck/issues/1827#issuecomment-485009538)) smo otkrili da OWASP Dependency-Check izaziva lažnu uzbunu za verzije Spring-a nakon v5.0.5.

* 1. spring-rabbit-2.2.6.RELEASE.jar *(Severity: medium)*

- Istraživanje prijavljenih ranjivosti nas je dovelo do informacija da je potrebno *update*-ovati verzije *dependency*-ja unutar gore navedenog, konkretno RabbitMQ amqp-client na verziju iznad v5.4.0 i Spring-AMQP na verziju iznad v2.0.6.RELEASE.

- Pošto mi koristimo RabbitMQ amqp-client v5.7.3 i Spring-AMQP v2.2.6.RELEASE, prijavljene ranjivosti predstavljaju lažnu uzbunu, kao i u prethodnom slučaju.

Frontend

* Za analizu Angular *dependency*-ja korišćenih u Agentskoj aplikaciji i u mikroservisima, upotrebili smo [npm audit](https://docs.npmjs.com/auditing-package-dependencies-for-security-vulnerabilities) komandu koja postoji unutar NPM (Node Package Manager-a) za Node.js pakete.
* Izveštaji dobijeni pomoću ove komande (pre intervencija): [Link](https://drive.google.com/drive/folders/18vPNtmFS1JtS93RTj2nLWPWab2zM_ZIO?usp=sharing)
* Kao što vidimo, uz svaku prijavljenu ranjivost data je i komanda za *update*-ovanje problematičnog *dependency*-ja, koje smo mi i upotrebili. Na taj način smo otklonili prijavljene ranjivosti.
* Međutim, komanda *npm install --save-dev @angular-devkit/build-angular@0.901.7*, iako je otklonila prijavljenu ranjivost vezanu za Yargs parser, onemogućila je pokretanje Angular aplikacije zbog nekompatibilnosti sa samom verzijom Angular *framework*-a koji koristimo. Iz tog razloga smo vratili prvobitnu verziju *angular-devkit/build-angular dependency*-ja, koji poseduje ranjivost.
* Prijavljena ranjivost Yargs parsera omogućuje *prototype pollution* napad. Zbog nedovoljno dobre sanitizacije, napadač je u mogućnosti da modifikuje Object prototip, što bi posledično izmenilo *property*-je svih postojećih objekata. To napadaču omogućava da ubaci i izvrši maliciozan kod nad svim postojećim objektima.
* Na primer, kada bi napadač uspeo da izmeni objekat koji predstavlja rolu, bio bi u mogućnosti da pristupi stranicama koje nisu dozvoljene roli koju on poseduje. Međutim, pošto se backend ne oslanja na role prosleđene sa frontend-a, napadač ne bi uspeo da na taj način ozbiljnije ugrozi celokupan sistem.
* Pošto je u pitanju *low severity* ranjivost za čiju je zloupotrebu neophodno da napadač poseduje kontrolu nad argumetima koji se Yargs parseru prosleđuju ([link](https://www.npmjs.com/advisories/1500)), odlučili smo se da ne preduzimamo nikakve dalje korake u vezi sa njom.