Uklanjanje ranjivosti na frontendu ništagrama

Za skeniranje ranjivosti na frontendu ništagrama je korišćena ugrađena npm komanda npm audit. Nakon pokretanja naredbe kao izveštaj dobili smo 55 ranjivosti (45 moderate I 10 high).

```
55 vulnerabilities (45 moderate, 10 high)

To address issues that do not require attention, run:
  npm audit fix
```

Figure 1: Izveštaj dobijen od strane npm audit komande

Glavni krivci za ove ranjivosti jesu paketi koji se nalaze u hijerarhiji dependencyja instaliranih paketa a to su: css-what, glob-parent, normalize-url, postcss, serialize-javascript I ssri.

```
css-what  <5.0.1
Severity: high
Denial of Service - https://npmjs.com/advisories/1754
fix available via `npm audit fix`
node_modules/svgo/node_modules/css-what
```

Figure 2: Deo npm audit izveštaja vezan za css-what paket

```
glob-parent  <5.1.2
Severity: moderate
Regular expression denial of service - https://npmjs.com/advisories/1751
fix available via `npm audit fix --force`
Will install @vue/cli-service@3.5.3, which is a breaking change
```

Figure 3: Deo npm audit izveštaja vezan za glob-parent paket

```
normalize-url  <=4.5.0 || 5.0.0 - 5.3.0 || 6.0.0
Severity: high
Regular Expression Denial of Service - https://npmjs.com/advisories/1755
fix available via `npm audit fix --force`
```

Figure 4: Deo npm audit izveštaja vezan za normalize-url paket

```
postcss  7.0.0 - 8.2.9
Severity: moderate
Regular Expression Denial of Service - https://npmjs.com/advisories/1693
fix available via `npm audit fix --force`
```

Figure 5: Deo npm audit izveštaja vezan za postcss paket

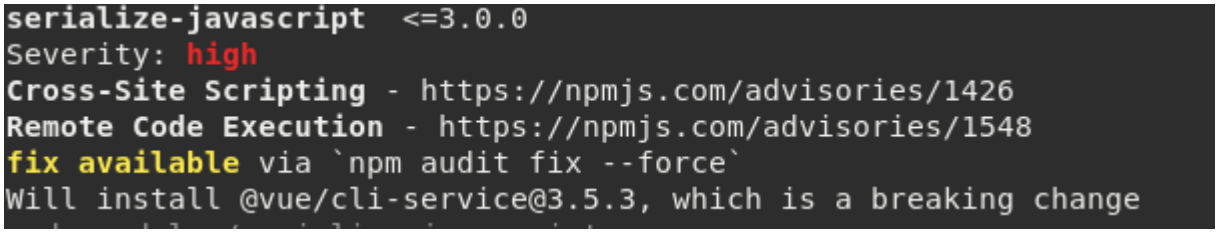

Figure 6: Deo npm audit izveštaja vezan za serialize-javascript paket

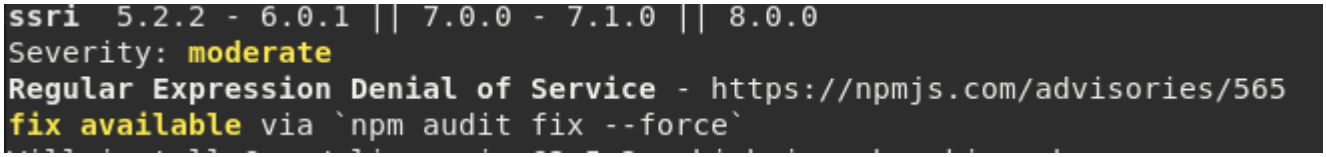

Figure 7: Deo npm audit izveštaja vezan za ssri paket

Pokretanjem npm audit i npm audit –fix komandi nismo dobili nikakva poboljšanja pa je za ispravljanje ranjivosti iskorišten dependency resolution koji forsira instalaciju specifičnih verzija paketa u celoj hijerarhiji dependency-ja.

Kako bi saznali verzije navedenih paketa koje nisu ranjive, pretražili smo bazu sajta snyk.io, a u sekciji resolutions package.json fajla ih pobrojali.

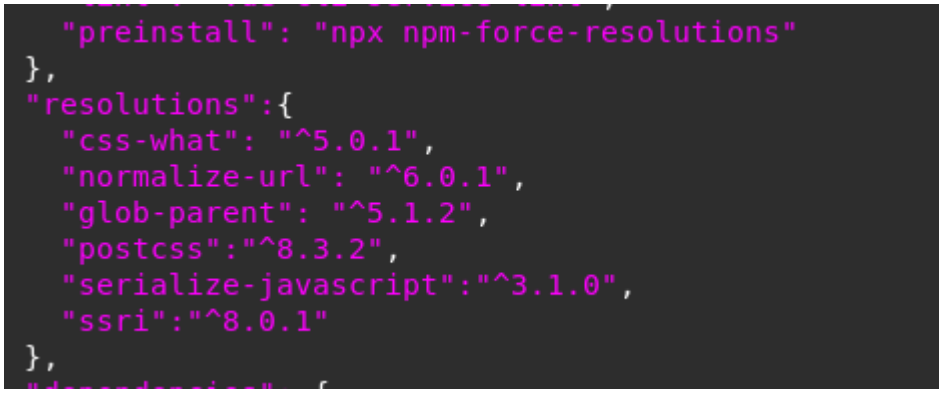

Figure 8: Resolutions sekcija package.json fajla

Nakon brisanja node_modules foldera i ponovne npm install komande, kao rezultat smo dobili 0 ranjivih paketa.

Figure 9: Rezultat npm audit komande nakon ispravljenih dependency-ja