Izveštaj

Kako bismo istakli temeljnost analize svih third-party komponenti na koje se naš sistem oslanja, za detektovanje poznatih ranjivosti u okviru dependency-ja koristili smo OWASP Dependency Check. Takođe, prilikom uključivanja svih korišćenih biblioteka, Vue.js nas je obavestio o potencijalnim ranjivostima koje smo analizirali.

Koristeći OWASP Dependency Check skenirano je 162 dependency-ja (120 jedinstvenih). Od njih, 4 su „vulnerable dependencies“ (ranjiva):

1. Dependency-check-core-5.2.2.jar: jquery-3.4.1.min.js

   Ponekad može da dovede do XSS napada, međutim ozbiljnost rizika je ocenjena kao srednja.

   Bitno je napomenuti da je verzija jQuery 3.5.0 uvela security fix (uz koji je neophodno izmeniti kod) koja na taj način smanjuje XSS ranjivost. Međutim, ona je i dalje prisutna.

2. Plexus-utils-3.0.22.jar

   Može da dovede do XML Injection napada, a ozbiljnost rizika je za sada nepoznata.

   Istražujući ovu ranjivost, došli smo do zaključka da je bitno ograničiti sadržaj koji se unosi u polja i tako sprečiti napadača da pristupi bazi i dođe do svih podataka koji se nalaze u njoj. Na taj način smo korisnicima onemogućili da izvršavaju upite koji mogu dovesti do toga.

3. Spring-security-core-5.3.2.RELEASE .jar

   Može dovesti do Incorrect Authorization. Spring Framework, u kombinaciji sa bilo kojim Spring Security-jem, sadrži Authorization Bypass kada se koriste security metode. U tom slučaju, neautentifikovani korisnik može zadobiti pristup metodama koje bi trebalo da su mu zabranjene.

   Ovu ranjivost rešili smo implementiranjem RBAC (Role Based Access Control). Neautentifikovani korisnici nemaju rolu, ne mogu da pristupe metodama koje su im zabranjene i samim tim ne mogu da obavljaju funkcionalnosti.

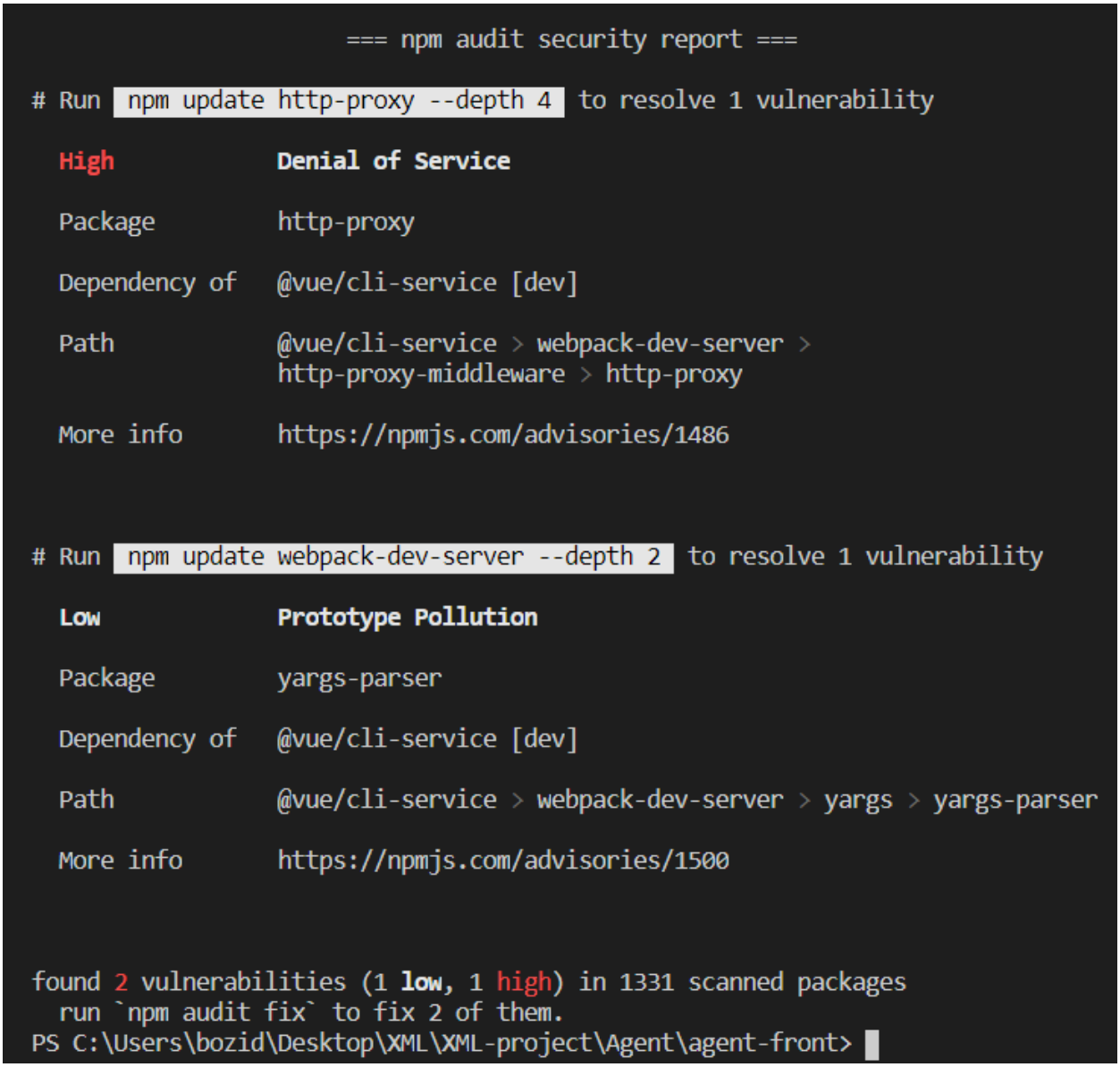
4. Spring-ws-support-2.1.4.RELEASE.jar

   Zbog starijih verzija može da dozvoli XXE Injection napade.

   XXE Injection je ranjivost web security-ja koja omogućava napadaču da se meša u obradu XML podataka aplikacije.

   Ovaj problem je rešiv korišćenjem novijih verzija.

Od 1331 skeniranog paketa, pronađene su 2 ranjivosti na frontendu. Vue.js nam nudi npm audit fix što može rešiti ove dve ranjivosti.



Slika 1 Frontend ranjivost

1. Denial of Service

   Verzije koje su prethodile verziji 1.18.1 pokazuju ranjivost na Denial of Service. Ozbiljnost rizika je ocenjena kao visoka. Iz tog razloga, unapređivanjem http-proxy-ja, sprečili smo ovaj problem.

2. Prototype Pollution

   Ukoliko argumenti nisu ispravno sanirani, napadač može da modifikuje prototip Objekta uzrokujući dodavanje ili modifikaciju postojećeg svojstva koje sadrže svi objekti. Ozbiljnost rizika je ocenjena kao niska.

   Vue.js nudi mogućnost rešavanja ove ranjivosti unapređivanjem webpack-dev-server-a.