Raport Audit de Vulnerabilități - Front-End (Angular)

Proiect: EPERS Front-End
Versiune: 1.0.0
Data generării raportului: 16.07.2025
Tool utilizat: `npm audit`

Rezumat

În urma rulării comenzii `npm audit` asupra proiectului **epers-front-end**, nu au fost identificate vulnerabilități cunoscute în pachetele utilizate la data scanării.

Comanda utilizată:

npm audit

Rezultat:
found 0 vulnerabilities

Detalii Pachete Utilizate

Mai jos este listată configurația completă a pachetelor utilizate, conform fișierului `package.json`:

Dependencies

Pachet	Versiune
@angular/animations	^20.1.0
@angular/cdk	^20.1.0
@angular/common	^20.1.0
@angular/compiler	^20.1.0
@angular/core	^20.1.0
@angular/forms	^20.1.0
@angular/material	^20.1.0
@angular/platform-browser	^20.1.0

@angular/platform-browser-dynamic	^20.1.0
@angular/router	^20.1.0
@ngneat/until-destroy	^10.0.0
@popperjs/core	^2.11.8
bootstrap	^5.3.7
chart.js	^4.5.0
ngx-toastr	^19.0.0
rxjs	^7.8.2
tslib	^2.8.1
zone.js	^0.15.1

DevDependencies

Pachet	Versiune
@angular/build	^20.1.0
@angular/cli	~20.1.0
@angular/compiler-cli	^20.1.0
@types/jasmine	^5.1.8
jasmine-core	^5.8.0
karma	^6.4.4
karma-chrome-launcher	^3.2.0
karma-coverage	^2.2.1
karma-jasmine	^5.1.0
karma-jasmine-html-reporter	^2.1.0
typescript	^5.8.3

Concluzie

Pe baza scanării efectuate cu `npm audit`, nu au fost identificate vulnerabilități cunoscute în pachetele utilizate în proiectul Angular.

Recomandare:

- Se recomandă rularea periodică a comenzilor `npm audit` și actualizarea constantă a pachetelor pentru a preveni expunerea la noi vulnerabilități.
- În cazul adăugării de noi pachete, se recomandă includerea verificărilor de securitate ca parte din pipeline-ul de CI/CD.