Raport Audit de Vulnerabilități - Back-End (.NET)

Proiect: EPERS Back-End
Framework: .NET 8.0
Data generării raportului: 16.07.2025
Tool utilizat: `dotnet list package –vulnerable`

Rezumat

În urma rulării comenzii:

dotnet list package --vulnerable

nu au fost identificate vulnerabilități cunoscute în pachetele utilizate, conform sursei oficiale: **https://api.nuget.org/v3/index.json**

The given project `EpersBackend` has no vulnerable packages given the current sources.
The given project `Epers.DataAccess` has no vulnerable packages given the current sources.
The given project `Epers.Models` has no vulnerable packages given the current sources.

Detalii Pachete Utilizate

Proiect: EpersBackend

Pachet	Versiune Solicitată	Versiune Instalată
AutoMapper.Extensions.Microsoft.DependencyInjection	12.0.1	12.0.1
ClosedXML	0.105.0	0.105.0
Microsoft.AspNetCore.Authentication.JwtBearer	8.0.18	8.0.18
Microsoft.AspNetCore.OpenApi	8.0.18	8.0.18
Microsoft.EntityFrameworkCore.Design	8.0.18	8.0.18
NETCore.MailKit	2.1.0	2.1.0
Newtonsoft.Json	13.0.3	13.0.3
QuestPDF	2025.7.0	2025.7.0
Serilog.AspNetCore	8.0.3	8.0.3
Swashbuckle.AspNetCore	8.1.4	8.1.4

Proiect: Epers.DataAccess

Pachet	Versiune Solicitată	Versiune Instalată
Microsoft.EntityFrameworkCore	8.0.18	8.0.18
Microsoft.EntityFrameworkCore.SqlServer	8.0.18	8.0.18

Proiect: Epers.Models

- **Pachete instalate:** *Nu există pachete de tip NuGet pentru acest proiect.*

Concluzie

Conform scanării efectuate cu `dotnet list package --vulnerable`, nu au fost identificate vulnerabilități în pachetele utilizate în proiectele backend ale aplicației EPERS.

Recomandări

- Se recomandă rularea periodică a comenzii `dotnet list package --vulnerable` pentru a menține siguranța pachetelor utilizate.
- Se recomandă includerea acestei verificări în pipeline-ul de CI/CD pentru a detecta rapid eventualele vulnerabilități apărute în timp.