IZVEŠTAJ O PROCENI BEZBEDNOSTI I RANJIVOSTI

Naziv projekta: bsep-ra-2024-kt2-tim-12
Datum: 15.06.2024.
Autor: Srđan Petronijević RA 201/2020
Verzija: 1.0

Pregled sadržaja:

1. UVOD

1.1 Svrha

Svrha ovog dokumenta je da izvrši sveobuhvatnu analizu svih third-party komponenti koje su korišćene u izradi aplikacije počevši od operativnog sistema, backend biblioteka, npm paketa I ostalih dependency.

2. OPSEG ANALIZE

2.1 Komponente uključene u analizu:

- Operativni sistem: GNU/Linux
- Distribucija: Fedora 40
- Backend: .NET Core 7.0
- Frontend: Angular 17.3.2
- Baza podataka: PostgreSQL 16
- Alati za razvoj: Node.js 20.12.2, npm 10.5.0, NuGet, Entity Framework 7.0.18

3. Metodologija

Za analizu ranjivosti korišćen je OWASP Dependency Check alat. Alat vrši analizu .NET I Node.js paketa.

4. Skupljanje Podataka

Identifikovane su sve komponente koje se koriste u aplikaciji i prikupiljeni su podaci o njihovim verzijama. Potom je izvršeno skeniranje koristeći navedeni alat i prikupljeni su izveštaji o ranjivostima.

5. ANALIZA RANJIVOSTI

- **Komponenta: Npgsql.EntityFrameworkCore.PostgreSQL.dll**
  - **Namena**: postgresql provajder za entity framework core
  - **Id ranjivosti:** Količina ranjivosti je prevelika da bi sve bile pobrojane ovde.
  - **Rešenje:** ne koristiti starije verzije postgresql. Verzija 9 je minsko polje.

- **Komponenta: braces**
  - **Namena:** proširenje zagrada nalik na bash u javascript programskom jeziku.
  - **Id ranjivosti:** CVE-2024-4068
  - **Opis ranjivosti:** verzije pre 3.0.3 ne uspevaju da ograniče broj karatketra koji mogu da podrže, što može dovesti do iscrpljenja memorije.
  - **Rešenje:** koristiti noviju verziju paketa
- **Komponenta: micromatch**
  - **Namena:** glob matching za javascript/node.js
  - **Id ranjivosti:** CVE-2024-4067
  - **Opis ranjivosti:** paket je ranjiv na regular expression denial of service(ReDos). U micromatch() metodi dolazi kada se koristi '*' obrazac kada on pohlepno odgovara bilo čemu. Prenošenjem zlonamernog korisnog payload-a, podudaranje šablona će nastaviti da se vraća nazad do ulaza dok ne pronađe zagradu za zatvaranje. Kako se veličina unosa povećava, vreme potrošnje će se takođe povećavati sve dok aplikacija ne visi ili uspori.
  - **Rešenje:** koristiti bezbedni obrazac koji neće početi da vraća nazad regularni izraz zbog pohlepnog podudaranja.
- **Komponenta: dotnet-aspnet-codegenerator-design.dll**
  - **Namena:** alat korišćen za generisanje koda u ASP.NET Core.

- **Komponenta: Microsoft.VisualStudio.Web.CodeGeneration.dll**
  - **Namena:** CodeGenCommand pronalazi prikladan generator koda I poziva ga iz projektnih dependency
- **Komponenta: Microsoft.VisualStudio.Web.CodeGeneration.EntityFrameworkCore.dll**

- **Namena:** OR maper za ASP.NET Core

- **Komponenta: Microsoft.CodeAnalysis.Razor.dll**
  - **Namena:** markup sintaksa za dodavanje server-side logike web stranicama
  - **Id ranjivosti:** CVE-2023-44487
  - **Opis ranjivosti:** HTTP/2 protokol omogućuje denial of service napad jer otkazivanje zahteva može da resetuje više tokova odjednom
  - **Rešenje:** koristiti verzije asp.net core od: 6.0.23, 7.0.12, .net od: 6.0.23, 7.0.12, node.js verzije od: 18.18.2, 20.8.1

- **Komponente (deljene ranjivosti): Microsoft.CodeAnalysis.Razor.dll, Microsoft.VisualStudio.Web.CodeGeneration.EntityFrameworkCore.dll, Microsoft.VisualStudio.Web.CodeGeneration.dll**
  - **Id ranjivosti:** CVE-2024-21386
  - **Opis ranjivosti:** .NET denial of service, CWE-400 nekontrolisano korišćenje resursa
  - **Rešenje:** koristiti asp.net core verzije od: 6.0.27, 7.0.16 I 8.0.2
  - **Id ranjivosti:** CVE-2024-21404
  - **Opis ranjivosti:** .NET denial of service, CWE-476 NULL dereferenciranje null pokazivača
  - **Rešenje:** koristiti asp.net core verzije od: 6.0.27, 7.0.16 I 8.0.2
  - **Id ranjivosti:** CVE-2023-36558
  - **Opis ranjivost:** ASP.NET Core zaobilaženje bezbednosnih funkcija
  - Rešenje: koristiti asp.net core verzije od: 6.0.25, 7.0.14

- **Komponenta: Fedora Linux**
  - **Namena**: GNU/Linux distribucija
  - **Id ranjivosti:** CVE-2024-37051
  - **Opis ranjivosti:** github access token moze biti izložen third-party sajtovima u JetBrains IDE
  - **Rešenje:** koristiti ide verzija: pre 2023.1 I posle: DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4

6. Izveštaj

Izveštaj generisan pomoću OWASP Dependency-Check se nalazi u prilogu. Sadrži detalje o identifikovanim ranjivostima, njihove CVE brojeve, opise i preporuke za rešavanje.

7. Završne Napomene

Ova analiza značajno poboljšava sigurnost aplikacije. Planiramo redovno ažuriranje (no cap) i reviziju bezbednosti svih komponenti u budućnosti kako bismo osigurali visok nivo sigurnosti.

8. Prilog

8.1 Dependency check

Izveštaj alata se nalazi u dependency-check-report.html fajlu.

8.2 Tabela ranjivosti

Dependency	ID ranjivosti	Paket	Ozbiljnost	CVE broj	Pouzdaost	Broj dokaza
Microsoft.CodeAnalysis.Razor.dll	cpe:2.3:a:microsoft:.net_core:6.0.11:*:*:*:*:*:*:* cpe:2.3:a:microsoft:asp.net:6.0.11:*:*:*:*:*:*:* cpe:2.3:a:microsoft:asp.net_core:6.0.11:*:*:*:*:*:*:*	pkg:generic/Microsoft.CodeAnalysis.Razor@6.0.11	VISOKA	4	NISKA	12
Microsoft.VisualStudio.Web.CodeGeneration.Core.dll	cpe:2.3:a:microsoft:asp.net_core:7.0.12:*:*:*:*:*:*:*	pkg:generic/Microsoft.VisualStudio.Web.CodeGeneration.Core@7.0.12	VISOKA	3	NISKA	13
Microsoft.VisualStudio.Web.CodeGeneration.EntityFrameworkCore.dll	cpe:2.3:a:microsoft:.net_core:7.0.12:*:*:*:*:*:*:* cpe:2.3:a:microsoft:asp.net:7.0.12:*:*:*:*:*:*:* cpe:2.3:a:microsoft:asp.net_core:7.0.12:*:*:*:*:*:*:*	pkg:generic/Microsoft.VisualStudio.Web.CodeGeneration.EntityFrameworkCore@7.0.12	VISOKA	3	NISKA	11
Microsoft.VisualStudio.Web.CodeGeneration.dll	cpe:2.3:a:microsoft:asp.net:7.0.12:*:*:*:*:*:*:*	pkg:generic/Microsoft.VisualStudio.Web.CodeGeneration@7.0.12	VISOKA	3	NISKA	11

	cpe:2.3:a:microsoft:asp.net_core:7.0.12:*:*:*:*:*:*:*					
Npgsql.EntityFrameworkCore.PostgreSQL.dll	cpe:2.3:a:postgresql:postgresql:7.0.11:*:*:*:*:*:*:* cpe:2.3:a:www-sql_project:www-sql:7.0.11:*:*:*:*:*:*:*	pkg:generic/Npgsql.EntityFrameworkCore.PostgreSQL@7.0.11	KRITIČNA	35	NAJVIŠA	15
braces:3.0.2	cpe:2.3:a:braces_project:braces:3.0.2:*:*:*:*:*:*:*	pkg:npm/braces@3.0.2	VISOKA	1	NAJVIŠA	8
dotnet-aspnet-codegenerator-design.dll	cpe:2.3:a:microsoft:.net_core:7.0.12:*:*:*:*:*:*:* cpe:2.3:a:microsoft:asp.net:7.0.12:*:*:*:*:*:*:* cpe:2.3:a:microsoft:asp.net_core:7.0.12:*:*:*:*:*:*:*		VISOKA	3	NAJVIŠA	9
micromatch:4.0.5		pkg:npm/micromatch@4.0.5	SREDNJA	1		8
Fedora Linux	https://www.cvedetails.com/cve/CVE-2024-37051/		KRITICNA			

8.3 Izvori

OWASP Dependency Check https://github.com/jeremylong/DependencyCheck
SAR Template https://ipkeys.com/blog/sar-template/
National Vulnerability Database: https://www.nist.gov/
OSS index: https://ossindex.sonatype.org/
Fedora Linux Vulnerabilities: https://www.cvedetails.com/vulnerability-list/vendor_id-6924/product_id-16334/Fedoraproject-Fedora.html