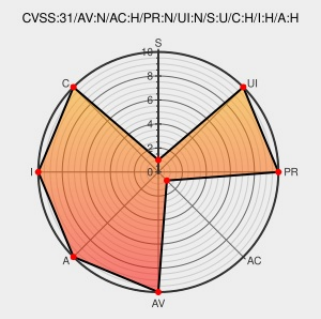
CVE-2022-24815

Published on: Not Yet Published

Last Modified on: 04/19/2022 05:34:00 PM UTC

CVE-2022-24815 - advisory for GHSA-qjmq-8hjr-qcv6

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Generator-jhipster from Jhipster contain the following vulnerability:

JHipster is a development platform to quickly generate, develop, & deploy modern web applications & microservice architectures. SQL Injection vulnerability in entities for applications generated with the option "reactive with Spring WebFlux" enabled and an SQL database using r2dbc. Applications created without "reactive with Spring WebFlux" and applications with NoSQL databases are not affected. Users who have generated a microservice Gateway using the affected version may be impacted as Gateways are reactive by default. Currently, SQL injection is possible in the findAllBy(Pageable pageable, Criteria criteria) method of an entity repository class generated in these applications as the where clause using Criteria for queries are not sanitized and user input is passed on as it is by the criteria. This issue has been patched in v7.8.1. Users unable to upgrade should be careful when combining criterias and conditions as the root of the issue lies in the `EntityManager.java` class when creating the where clause via `Conditions.just(criteria.toString())`. `just` accepts the literal string provided. Criteria's `toString` method returns a plain string and this combination is vulnerable to sql injection as the string is not sanitized and will contain whatever used passed as input using any plain SQL.

CVE-2022-24815 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **jhipster** - **generator-jhipster** version **>= 7.0.0, < 7.8.1**

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SQL Injection when creating an application with Reactive SQL backend · Advisory · jhipster/generator-jhipster · GitHub	github.com text/html	CONFIRM github.com/jhipster/generator-jhipster/security/advisories/GHSA-qjmq-8hjr-qcv6
use conditions instead of criteria as workaround · jhipster/generator-jhipster@c220a21 · GitHub	github.com text/html	MISC github.com/jhipster/generator-jhipster/commit/c220a210fd7742c53eea72bd5fadbb96220faa98
SQL Injection in Reactive project · Issue #18269 · jhipster/generator-jhipster · GitHub	github.com text/html	MISC github.com/jhipster/generator-jhipster/issues/18269

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jhipster	Generator-jhipster	All	All	All	All

cpe:2.3:a:jhipster:generator-jhipster:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@jhipster	JHipster v7.8.1 released to address CVE-2022-24815 The SQL Injection vulnerability affects reactive apps/gateways… twitter.com/i/web/status/1…	2022-04-07 06:28:36
@ipssignatures	The vuln CVE-2022-24815 has a tweet created 0 days ago and retweeted 10 times. twitter.com/jhipster/statu… #pow1rtrtwwcve	2022-04-07 10:06:00
@CVEreport	CVE-2022-24815 : JHipster is a development platform to quickly generate, develop, & deploy modern web applications… twitter.com/i/web/status/1…	2022-04-11 19:26:03
/r/netcve	CVE-2022-24815	2022-04-11 20:38:39

← Previous ID

Next ID→