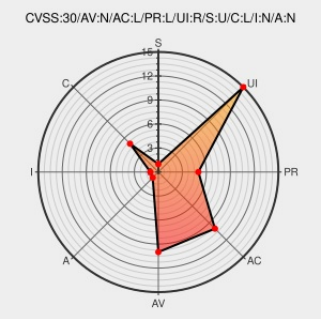
CVE-2019-3797

Published on: 05/06/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:43 PM UTC

CVE-2019-3797

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



Certain versions of Spring Data Java Persistence Api from Pivotal Software contain the following vulnerability:

This affects Spring Data JPA in versions up to and including 2.1.5, 2.0.13 and 1.11.19. Derived queries using any of the predicates ‘startingWith’, ‘endingWith’ or ‘containing’ could return more results than anticipated when a maliciously crafted query parameter value is supplied. Also, LIKE expressions in manually defined queries could return unexpected results if the parameter values bound did not have escaped reserved characters properly.

CVE-2019-3797 has been assigned by security_alert@emc.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Spring** - **Spring Boot** version **v2.0.9.RELEASE**

Affected Vendor/Software: **Spring** - **Spring Boot** version **v1.5.20.RELEASE**

Affected Vendor/Software: **Spring** - **Spring Boot** version **v2.1.4.RELEASE**

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL | NONE | NONE

CVE References

Description	Tags	Link
CVE-2019-3797: Additional information exposure with Spring Data JPA derived queries | Security | Pivotal	Vendor Advisory pivotal.io text/html	CONFIRM pivotal.io/security/cve-2019-3797

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

981792 Java (maven) Security Update for org.springframework.data:spring-data-jpa (GHSA-jgmr-wrwx-mgfj)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pivotal Software	Spring Data Java Persistence Api	All	All	All	All
Application	Pivotal Software	Spring Data Java Persistence Api	All	All	All	All
Application	Pivotal Software	Spring Data Java Persistence Api	All	All	All	All

cpe:2.3:a:pivotal_software:spring_data_java_persistence_api:*:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring_data_java_persistence_api:*:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring_data_java_persistence_api:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→