



VDB-356374 · CVE-2026-5848 · ISSUE 4587

JEECGBOOT JIMUREPORT UP TO 2.3.0 DATA SOURCE TESTCONNECTION DRIVERMANAGER.GETCONNECTION DBURL CODE INJECTION

CVSS Meta Temp Score ?

4.5

Current Exploit Price (≈) ?

\$0-\$5k

CTI Interest Score ?

1.59

Summary

A vulnerability was found in [jeecgboot JimuReport up to 2.3.0](#) and classified as **critical**. The impacted element is the function `DriverManager.getConnection` of the file `/drag/onlDragDataSource/testConnection` of the component `Data Source Handler`. Executing a manipulation of the argument `dbUrl` can lead to code injection. The identification of this vulnerability is [CVE-2026-5848](#). The attack may be launched remotely. Furthermore, there is an exploit available. The vendor confirmed the issue and will provide a fix in the upcoming release.

Details

A vulnerability classified as **critical** was found in [jeecgboot JimuReport up to 2.3.0](#). This vulnerability affects the function `DriverManager.getConnection` of the file `/drag/onlDragDataSource/testConnection` of the component `Data Source Handler`. The manipulation of the argument `dbUrl` with an unknown input leads to a code injection vulnerability. The CWE definition for the vulnerability is [CWE-94](#). The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is available at [github.com](#). This vulnerability was named [CVE-2026-5848](#). The exploitation appears to be easy. The attack can be initiated remotely. Additional levels of successful authentication are needed for exploitation. Technical details and also a public exploit are known. This vulnerability is assigned to [T1059](#) by the MITRE ATT&CK project.

It is possible to download the exploit at [github.com](#). It is declared as proof-of-concept. The vendor confirmed the issue and will provide a fix in the upcoming release.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Product

Type

- Reporting Software

Vendor

- jeecgboot

Name

- JimuReport

Version

- 2.0
- 2.1
- 2.2
- 2.3.0



Website

- Product: <https://github.com/jeecgboot/jimureport/>

CPE 2.3

- 
- 
- 

CPE 2.2

- 
- 
- 

CVSSv4

VulDB Vector: 

VulDB Reliability: 

CVSSv3

VulDB Meta Base Score: 4.7

VulDB Meta Temp Score: 4.5

VulDB Base Score: 4.7

VulDB Temp Score: 4.5

VulDB Vector: 🔒

VulDB Reliability: 🔍

CVSSv2



VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Code injection

CWE: [CWE-94](#) / [CWE-74](#) / [CWE-707](#)

CAPEC: 🔒

ATT&CK: 🔒

Physical: No

Local: No

Remote: Yes

Availability: 🔒

Access: Public

Status: Proof-of-Concept

Download: 🔒

Price Prediction: 🔍

Current Price Estimation: 🔒



Threat Intelligence

Interest: 🔍

Active Actors: 🔍

Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known

Status: 🔍

0-Day Time: 🗝️

Timeline

04/08/2026	█		Advisory disclosed
04/08/2026	█	+0 days	VulDB entry created
04/08/2026	█	+0 days	VulDB entry last update

Sources

Product: github.com

Advisory: [4587](#)

Status: Confirmed

Confirmation: 🗝️

CVE: [CVE-2026-5848](#) (🗝️)

GCVE (CVE): [GCVE-0-2026-5848](#)

GCVE (VulDB): [GCVE-100-356374](#)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

Entry

Created: 04/08/2026 09:16 PM

Changes: 04/08/2026 09:16 PM (61)

Complete: 🔍

Submitter: [anch0r](#)

Cache ID: 172:CC2:179

Submit

Accepted

- [Submit #790769: jeeegboot jimureport <= 2.3.0 Code Injection \(by anch0r\)](#)

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)