COMMUNITY CONTENT

Home › Submit › 790769

Submit #790769: jeecgboot jimureport <= 2.3.0 Code Injection

Title	jeecgboot jimureport <= 2.3.0 Code Injection
Description	JimuReport (jimureport) v2.3.0 and earlier is vulnerable to Remote Code Execution (RCE) via the /drag/onlDragDataSource/testConnection endpoint. An authenticated attacker can supply a crafted H2 JDBC URL containing an INIT parameter that executes arbitrary SQL statements during the database connection process. By using CREATE ALIAS to define a Java function that calls Runtime.exec(), the attacker can execute arbitrary operating system commands on the server. The endpoint passes the user-supplied JDBC URL directly to DriverManager.getConnection() without adequate validation of H2-specific dangerous parameters such as INIT, RUNSCRIPT, or TRIGGER.
Source	⚠ https://github.com/jeecgboot/jimureport/issues/4587
User	anch0r (UID 96691)
Submission	03/27/2026 03:16 AM (13 days ago)
Moderation	04/08/2026 09:11 PM (13 days later)
Status	Accepted
VulDB entry	356374 [jeecgboot JimuReport up to 2.3.0 Data Source testConnection DriverManager.getConnection dbUrl code injection]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling