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 <=1.06 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

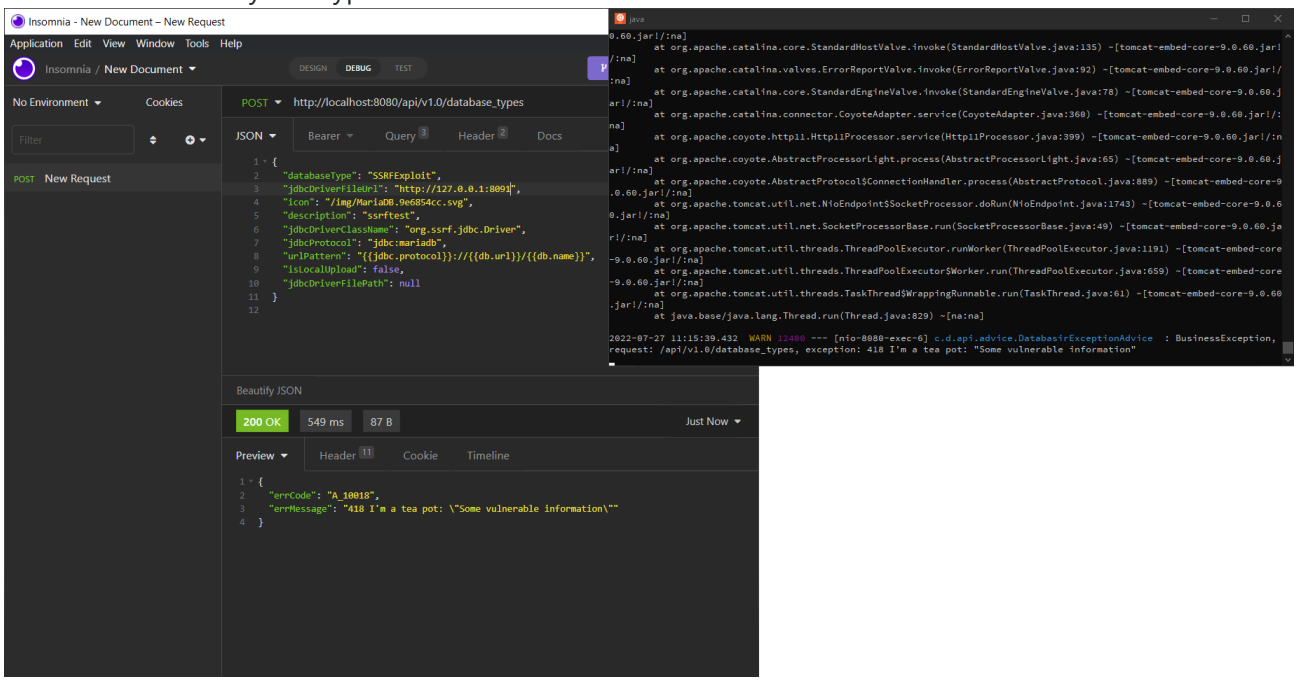
Are there any links users can visit to find out more?

For more information

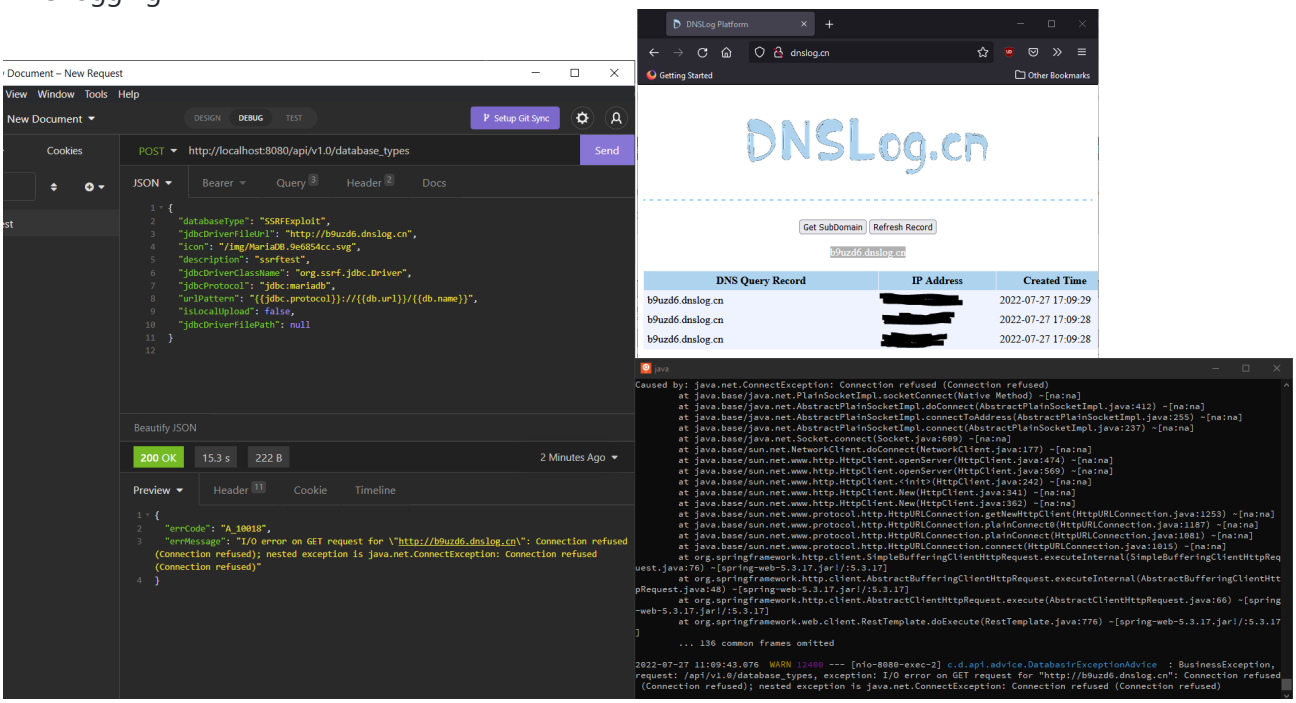
Example json payload for SSRF POST request to `/api/v1.0/database_types`

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

Proof of vulnerability honeypot



DNS logging



Databasir logging

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