Blind command injection in yogeshojha/rengine

3

Valid Reported on Apr 28th 2022

Description

Hello , its my first report in huntr.dev
fast code review : file
https://github.com/yogeshojha/rengine/blob/master/web/api/views.py#L820

```
class CMSDetector(APIView):
    def get(self, request):
        req = self.request
        url = req.query_params.get('url')
        #save_db = True if 'save_db' in req.query_params else False
        response = {'status': False}
        try:
            response = get_cms_details(url)
        except Exception as e:
            response = {'status': False, 'message': str(e)}
        return Response(response)
```

param : url
file 2 :
https://github.com/yogeshojha/rengine/blob/master/web/reNgine/common_func.py#L668

```
def get_cms_details(url):
    # this function will fetch cms details using cms_detector
    response = {}
    cms_detector_command = 'python3 /usr/src/github/CMSeeK/cmseek.py -u {}
    os.system(cms_detector_command)

    response['status'] = False
    response['message'] = 'Could not detect CMS!'
```

```
    parsed_url = urlparse(url)

    domain_name = parsed_url.hostname
    port = parsed_url.port

    find_dir = domain_name

    if port:
        find_dir += '_{}'.format(port)


    print(url)
    print(find_dir)
```

Proof of Concept

```
http:///api/tools/cms_detector/?format=json&url=ls;ls;ls
```

Impact

command injection

CVE
CVE-2022-1813
(Published)

Vulnerability Type
CWE-78: OS Command Injection

Severity
High (8.3)

Registry
Other

Affected Version
1.1

Visibility
Public

Status
Fixed

Found by

Ph33r
@ph33rr
unranked

This report was seen 818 times.

We are processing your report and will contact the **yogeshojha/rengine** team within 24 hours.
7 months ago

We have contacted a member of the **yogeshojha/rengine** team and are waiting to hear back
7 months ago

We have sent a follow up to the **yogeshojha/rengine** team. We will try again in 7 days.
7 months ago

We have sent a second follow up to the **yogeshojha/rengine** team. We will try again in 10 days.
7 months ago

A **yogeshojha/rengine** maintainer has acknowledged this report 6 months ago

Yogesh Ojha 6 months ago Maintainer

This is interesting. Working on the fix.

Yogesh Ojha gave praise 6 months ago

This was a great finding @ph33rr. I believe this deserves a CVE ID, please go ahead and initiate the process for CVE ID, and let me know if I could be of any help. Thank you

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

Yogesh Ojha validated this vulnerability 6 months ago

Ph33r has been awarded the disclosure bounty

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Yogesh Ojha marked this as fixed in **1.2.0** with commit **8277ce** 6 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Yogesh Ojha gave praise 6 months ago

This was a great finding @ph33rr. I believe this deserves a CVE ID, please go ahead and initiate the process for CVE ID, and let me know if I could be of any help. Thank you

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

Yogesh Ojha 6 months ago — Maintainer

@admin, how do I personally award the researcher bounty? I think we have exhausted the bounty amount for this month, so I would like to award him personally.

Thanks

Jamie Slome 6 months ago — Admin

@yogeshojha - this is certainly something I am sure we can help you with. Are you able to just send us an e-mail (`info@huntr.dev`) so that we can better process your request?

Sign in to join this conversation