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.

```
  9
 10
 11  # Get this theme's settings based on what was entered within its plugin.
 12  # This function is in functions.php
 13  $innov_settings = Innovation_Settings();
 14
 15  # Include the header template
 16  include('header.inc.php');
 17  ?>
 18
 19      <div class="wrapper clearfix">
 20          <!-- page content -->
 21          <article>
 22              <section>
 23
 24                  <!-- title and content -->
 25                  <h1><?php get_page_title(); ?></h1>
 26                  <?php get_page_content(); ?>
 27
 28                  <!-- page footer -->
 29                  <div class="footer">
 30                      <p>Published on <time datetime="<?php get_page_date('Y-m-d'); ?>" pubdate><?php get_page_date('F jS, Y'); ?></time>
 31                  </div>
 32              </section>
 33
 34          </article>
 35
 36          <!-- include the sidebar template -->
 37          <?php include('sidebar.inc.php'); ?>
 38      </div>
 39
 40  <!-- include the footer template -->
 41  <?php include('footer.inc.php'); ?>
```

Save Changes or Cancel

Request to http://localhost:80 [127.0.0.1]

| Forward | Drop | Intercept is on | Action | Open Browser |

Pretty Raw Hex

```
1  POST /simplecms/admin/theme-edit.php ?t=Innovation&f=template.php HTTP/1.1
2  Host: 127.0.0.1
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
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
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 1829
9  Origin: http://localhost
0  Connection: close
1  Referer: http://localhost/simplecms/admin/theme-edit.php
2  Cookie: __atuvc=3%7C38; __atuvs=632ec6d8828a5492002; GS_ADMIN_USERNAME=w0c4tool; 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
8
9  nonce=d2055326730a5f7b3c18fa32f5c54214bb3f195b &content=
   %3C%3Fphp+if%28%21defined%28%27IN_GS%27%29%29%7B+die%28%27you+cannot+load+this+page+directly.%27%29%29%3B+%7D%0D%0A%2F************
   *****************************************%0D%0A*%0D%0A*+%40File%3A+%09%09%09template.php%0D%0A+%40Package%3A%09%09GetSimple%0D%
   0A*+%40Action%3A%09%09Innovation+theme+for+GetSimple+CMS%0D%0A*%0D%0A*******************************************************%2F%0
   D%0A%0D%0A%0D%0A%23+Get+this+theme%27s+settings+based+on+what+was+entered+within+its+plugin.+%0D%0A%23+This+function+is+in+func
   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
   7header.inc.php%27%29%3B+%0D%0A%3F%3E%0D%0A%0D%0A%0D%0A%09%3Cdiv+class%3D%22wrapper+clearfix%22%3E%0D%0A%09%09%3C%21--+page+conten
   t+--%3E%0D%0A%09%09%09%3Carticle%3E%0D%0A%09%09%09%3Csection%3E%0D%0A%09%09%09%09%09%09%09%3C%21--+title+and+content+--%3
   E%0D%0A%09%09%09%09%3Ch1%3E%3C%3Fphp+get_page_title%28%29%3B+%3F%3E%3C%2Fh1%3E%0D%0A%09%09%09%09%3C%3Fphp+get_page_content%28%2
   9%3B+%3F%3E%0D%0A%09%09%09%09%0D%0A%09%09%09%09%3C%21--+page+footer+--%3E%0D%0A%09%09%09%09%3Cdiv+class%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
   php+get_page_date%28%27F+jS%2C+Y%27%29%3B+%3F%3E%3C%2Ftime%3E%3C%2Fp%3E%0D%0A%09%09%09%09%3C%2Fdiv%3E%0D%0A%09%09%09%3C%2Fsecti
   on%3E%0D%0A%09%09%09%0D%0A%09%09%3C%2Farticle%3E%0D%0A%09%09%09%09%3C%21--+include+the+sidebar+template+--%3E%0D%0A%09%09
   %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

Then we access index.php

👍 1

✏️ 🖥️ **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