Arbitrary code execution vulnerability exists in ESPCMS management system

Vulnerability description:

The vulnerability modifies the content of the homepage template file in the background, and after modification, a PHP suffix file with the same content will be generated. When the frontend accesses the homepage file, local code execution will be triggered.

Supplier: https://www.ecisp.cn/

Vulnerability file:

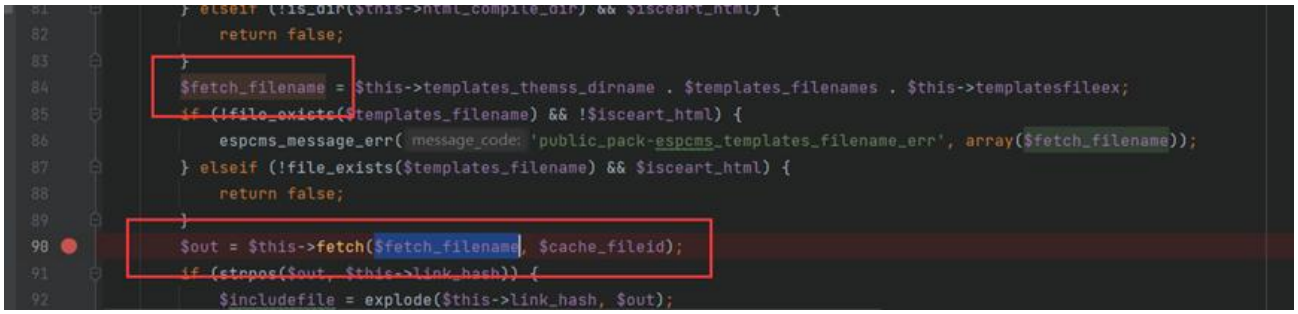
espcms\espcms_public\espcms_templates\ESPCMS_Templates.php

Code Analysis:

The code execution function eval is called in line 165. The content obtained by the $out variable is the content of the template file. The $fetch_filename parameter in line 84 is actually the address of the template file. In line 90, it is simply obtained with the file_get_contents() function. The contents of the template file are then assigned to $out.

espcms\espcms_public\espcms_templates\ESPCMS_Templates.php

```
155             }
156         } else {
157             if ($isceart_html) {
158                 ob_start();
159                 @eval('?' . '>' . trim($out));
160                 $content = ob_get_contents();
161                 ob_end_clean();
162                 ob_end_flush();
163                 return $this->cachefilewrite($htm_filename, $content);
164             } else {
165                 @eval('?' . '>' . trim($out));
166             }
167         }
168     }
169
170     private function format_js($str) {
```



```
82          return false;
83      }
84      $fetch_filename = $this->templates_themss_dirname . $templates_filenames . $this->templatesfileex;
85      if (!file_exists($templates_filename) && !$isceart_html) {
86          espcms_message_err( message_code: 'public_pack-espcms_templates_filename_err', array($fetch_filename));
87      } elseif (!file_exists($templates_filename) && $isceart_html) {
88          return false;
89      }
90      $out = $this->fetch($fetch_filename, $cache_fileid);
91      if (strpos($out, $this->link_hash)) {
92          $includefile = explode($this->link_hash, $out);
```

This function is a function to modify the content of the template file. There are user-controllable input parameters in line 174, and the content is written to the template file in line 211.

espcms\espcms_admin\control\TemplateFile.php

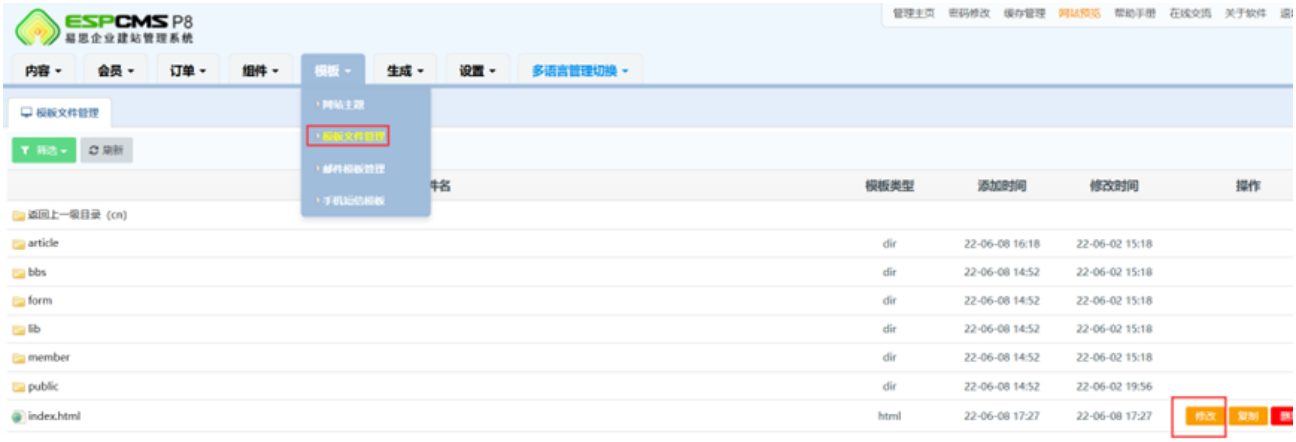
```
172             espcms_public_dialog( domid_name: 'espcms_public_dialog', message_code: 'public_pa
173         }
174         $content = $_POST['content'];
175         if (empty($content)) {
176             espcms_public_dialog( domid_name: 'espcms_public_dialog', message_code: 'public_pa
177         }
178         $template_dir_name = ESPCMS_Core::get_skin($open_type, return_key: 'skin_code');
179         $templates_dir = ESPCMS_FILE_ROOT . 'templates/' . $template_dir_name . '/';
180         $edit_file = $templates_dir . $open_path . '/' . $open_file;
181         $edit_path = $templates_dir . $open_path . '/';
```

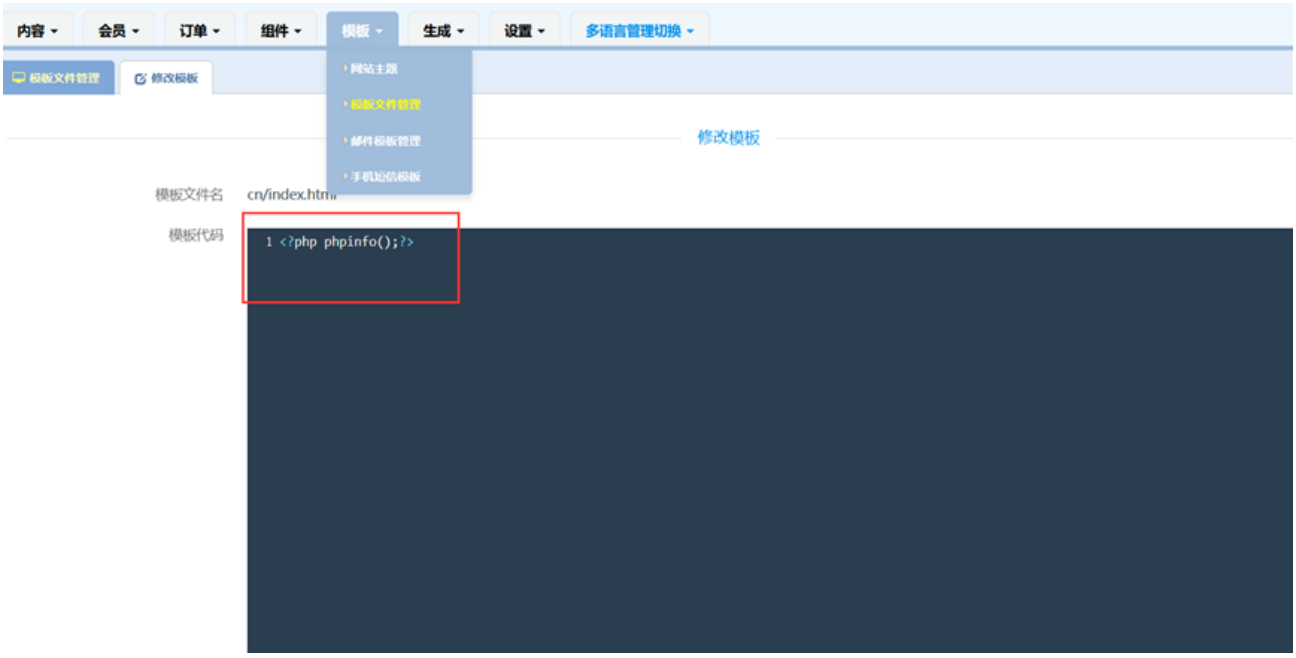
```
            $copy_file = $edit_path . $filename . '.' . $file_inof;
            $content = stripslashes($content);
            $install_id = ESPCMS_FileTool::writeFile($copy_file, $content);
            if (!$install_id) {
                espcms_public_dialog( domid_name: 'espcms_public_dialog', message_code: 'templates_pack-espcms_templates_
            }
            espcms_log_install( message_code: 'templates_pack-espcms_templates_file_button_copy', extras_message: $filename
            espcms_public_dialog( domid_name: 'espcms_info_save_ok', message_code: 'templates_pack-espcms_templates_file_
        } elseif ($saveType == 'edit') {
            $content = stripslashes($content);
            $update_id = ESPCMS_FileTool::writeFile($edit_file, $content);
            if (!$update_id) {
                espcms_public_dialog( domid_name: 'espcms_public_dialog', message_code: 'templates_pack-espcms_templates_
            }
            espcms_log_install( message_code: 'templates_pack-espcms_templates_file_button_edit', extras_message: $open_pat
            espcms_public_dialog( domid_name: 'espcms_info_save_ok', message_code: 'templates_pack-espcms_templates_file_
```

Steps to reproduce:

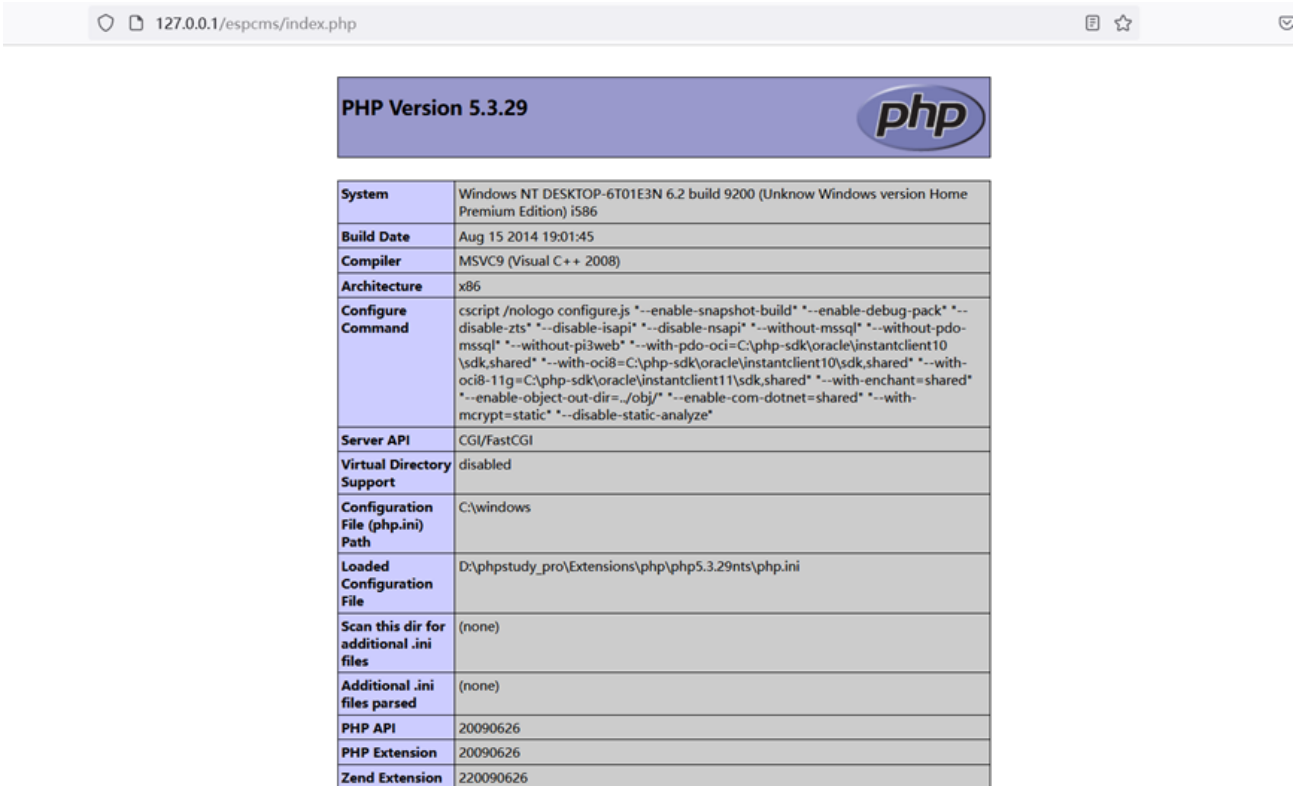
\1. Log in to the background management page as an administrator

\2. Click Template Management -> Modify and change the content to





\3. After the modification is successful, save it, and access the home page to cause the code to execute.



System	Windows NT DESKTOP-6T01E3N 6.2 build 9200 (Unknow Windows version Home Premium Edition) i586
Build Date	Aug 15 2014 19:01:45
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\windows
Loaded Configuration File	D:\phpstudy_pro\Extensions\php\php5.3.29nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626