

New issue

[Jump to bottom](#)

# There is an arbitrary file writing vulnerability in the HYBBS production plugin function #34

🔴 Open shmilylty opened this issue on Feb 7 · 0 comments

shmilylty commented on Feb 7 • edited ▼

## There is an arbitrary file writing vulnerability in the HYBBS production plugin function

### Vulnerability overview

There is an arbitrary file writing vulnerability in the HYBBS management background making plugin function, which leads to the server permission being obtained.

### Vulnerability scope

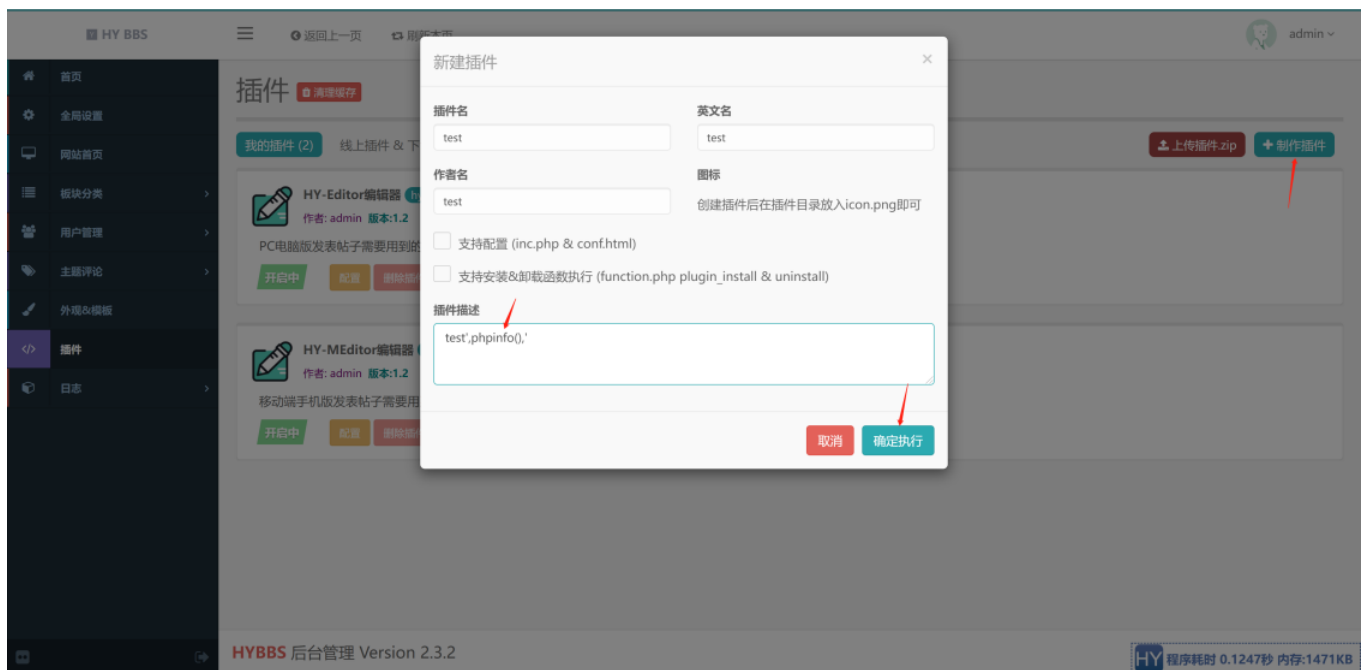
All versions prior to HYBBS 2.3.3

### Vulnerability environment construction

Clone the latest code factory library of HYBBS to the local, and then use phpstudy to build HYBBS.

### Vulnerability reproduction steps

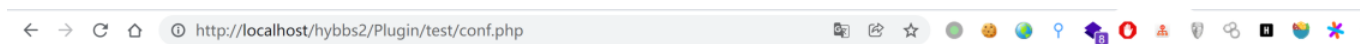
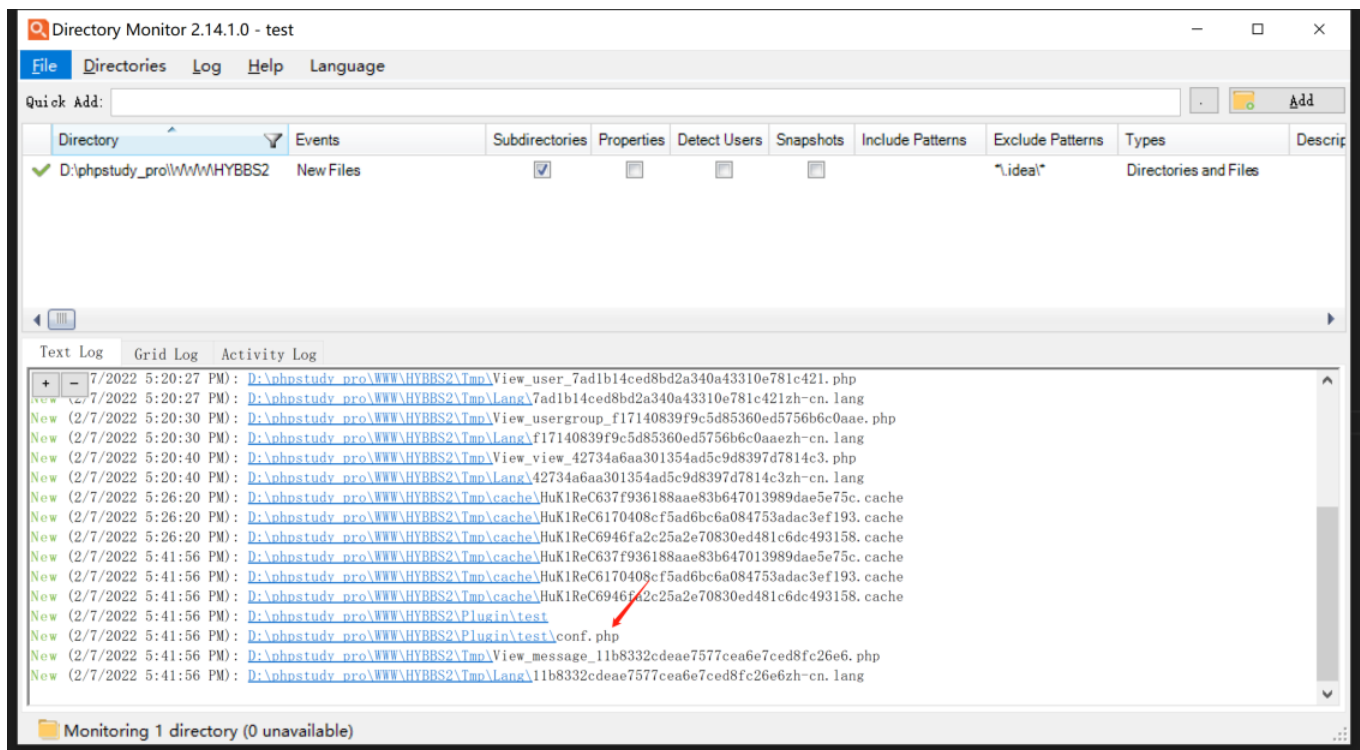
Fill in `test'`, `phpinfo()`, `'` in the plugin description, and click the OK button.




Then it will prompt that the plugin was created successfully



From the folder monitoring software log, you can see that the program created the malicious file conf.php





PHP Version 7.3.4	
	
System	Windows NT NC 10.0 build 19043 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=.\obj" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15
PHP Extension Build	API20180731,NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled

## Vulnerability code analysis

Locate the code that makes the plug-in function

```
1718 del_dir( dir: PLUGIN_PATH . "{$name}", bl: false, on_del: true);
1719 del_cache_file($this->conf);
1720 return $this->mess( a: '删除成功');
1721 }elseif($gn == 'add'){ //添加插件 建立插件目录
1722     $name = X( name: "post.name"); //插件名
1723     $name2 = X( name: "post.name2"); //插件英文名
1724     $user = X( name: "post.user"); //作者
1725     $icon = X( name: "post.icon"); //fa图标
1726     $mess = X( name: "post.mess"); //插件描述
1727     $inc = X( name: "post.inc"); //是否开启配置功能
1728     $fun = X( name: "post.fun"); //是否支持函数
1729
1730     if(is_dir( filename: PLUGIN_PATH . $name2))
1731         return $this->mess( a: "已存在相同英文名的插件");
1732     create_dir( path: PLUGIN_PATH . $name2);
1733     file_put_contents( filename: PLUGIN_PATH . $name2 . '/conf.php', data: "<?php
1734
1735     return array(
1736         'name' => '{$name}',
1737         'user' => '{$user}',
1738         'icon' => '{$icon}',
1739         'mess' => '{$mess}',
1740         'version' => '1.0',
1741     );");
1742
1743     if($inc){
1744         put_tmp_file( path: PLUGIN_PATH . $name2 . '/inc.php', content: '{}');
```

It can be seen that the program directly writes the plugin-related configuration information to conf.php without any security filtering, resulting in an arbitrary file writing vulnerability.

  shmilylty changed the title ~~There is an arbitrary file writing vulnerability in the HYBBS production plugin function~~ There is an arbitrary file writing vulnerability in the HYBBS production plugin function on Feb 7

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

