Discuz!X 前台任意文件删除漏洞深入解析

0r3ak / 2017-10-09 03:13:00 / 浏览数 7671 技术文章 技术文章 顶(0) 踩(0)

Author:0r3ak@0kee Team&&warlock@0kee Team

0x00 漏洞简介

漏洞名称：Discuz!X 前台任意文件删除

影响版本：全版本

危害等级：严重

0x01 Discuz!X路由解析

在说漏洞前，咱们可以先来学习一下Discuz的执行流程，其实已经有大佬把任意文件删除漏洞分析扔网上了，所以这里我顺带剖析一下discuz的运行原理，其实搞懂一个系

这里比较重要的是/source/目录，为程序模块功能函数，论坛所有的功能实现都要从主文件里面包含调用这里的模块来执行相应的操作
，/data/目录是附件数据、数据库与文件缓存，/api目录是第三方接口，包含了论坛的第三方接口文件，还有UCenter文件，这里也是漏洞常发文件，平时审计的时候也非常

不像现在大多数CMS系统使用流行开源框架在application里面来写Controller，Controller里面多个function，Discuz的服务端功能是以模块文件的形式来加载的

这里就拿系列漏洞触发的主文件home.php来看，home.php是论坛用户的个人中心文件：

```
<?php

/**
*      [Discuz!] (C)2001-2099 Comsenz Inc.
*      This is NOT a freeware, use is subject to license terms
*
*      $Id: home.php 32932 2013-03-25 06:53:01Z zhangguosheng $
*/

define('APPTYPEID', 1);
define('CURSCRIPT', 'home');

if(!empty($_GET['mod']) && ($_GET['mod'] == 'misc' || $_GET['mod'] == 'invite')) {
define('ALLOWGUEST', 1);
}

require_once './source/class/class_core.php';
require_once './source/function/function_home.php';

$discuz = C::app();

$cachelist = array('magic','userapp','usergroups', 'diytemplatenamehome');
$discuz->cachelist = $cachelist;
$discuz->init();

$space = array();

$mod = getgpc('mod');

if(!in_array($mod, array('space', 'spacecp', 'misc', 'magic', 'editor', 'invite', 'task', 'medal', 'rss', 'follow'))) {

$mod = 'space';

$_GET['do'] = 'home';

}

if($mod == 'space' && ((empty($_GET['do']) || $_GET['do'] == 'index') && ($_G['inajax']))) {
$_GET['do'] = 'profile';
}
$curmod = !empty($_G['setting']['followstatus']) && (empty($_GET['diy']) && empty($_GET['do']) && $mod == 'space' || $_GET['do
define('CURMODULE', $curmod);
runhooks($_GET['do'] == 'profile' && $_G['inajax'] ? 'card' : $_GET['do']);
```

```
require_once libfile('home/'.$mod, 'module');

?>
```

首先获取外部mod变量，也就是模块名称，接着对$mod进行gpc判断，再看$mod是否在数组里面的，是否是指定的space模块，最终带入到libfile解析出模块路径进行包

>POST /home.php?mod=spacecp&ac=profile&op=base
>data: affectivestatus=wwwwshph0r3ak

通过动态调试跟进去：（注：代码还是以编辑形式展示，红色代码段为phpstorm跟进的地方）

```
function libfile($libname, $folder = '') {
$libpath = '/source/'.$folder;
if(strstr($libname, '/')) {
list($pre, $name) = explode('/', $libname);
$path = "{$libpath}/{$pre}/{$pre}_{$name}";
} else {
$path = "{$libpath}/{$libname}";
}
return preg_match('/^[\w\d\/_]+$/i', $path) ? realpath(DISCUZ_ROOT.$path.'.php') : false;

}
```

这里libfile用于组合被包含文件的路径地址，从而包含执行目标文件，执行完后直接跳到/source/module/home/home_spacecp.php，前面一步可以看作是一个功能模

```
if(!defined('IN_DISCUZ')) {
exit('Access Denied');
}

require_once libfile('function/spacecp');
require_once libfile('function/magic');

$acs = array('space', 'doing', 'upload', 'comment', 'blog', 'album', 'relatekw', 'common', 'class',
'swfupload', 'poke', 'friend', 'eccredit', 'favorite', 'follow',
'avatar', 'profile', 'theme', 'feed', 'privacy', 'pm', 'share', 'invite','sendmail',
'credit', 'usergroup', 'domain', 'click','magic', 'top', 'videophoto', 'index', 'plugin', 'search', 'promotion');

$_GET['ac'] = $ac = (empty($_GET['ac']) || !in_array($_GET['ac'], $acs))?'profile':$_GET['ac'];
$op = empty($_GET['op'])?'':$_GET['op'];
if(!in_array($ac, array('doing', 'upload', 'blog', 'album'))) {
$_G['mnid'] = 'mn_common';
}

if($ac != 'comment' || !$_G['group']['allowcomment']) {
if(empty($_G['uid'])) {
if($_SERVER['REQUEST_METHOD'] == 'GET') {
dsetcookie('_refer', rawurlencode($_SERVER['REQUEST_URI']));
} else {
dsetcookie('_refer', rawurlencode('home.php?mod=spacecp&ac='.$ac));
}
showmessage('to_login', '', array(), array('showmsg' => true, 'login' => 1));
}

$space = getuserbyuid($_G['uid']);
if(empty($space)) {
showmessage('space_does_not_exist');
}
space_merge($space, 'field_home');

if(($space['status'] == -1 || in_array($space['groupid'], array(4, 5, 6))) && $ac != 'usergroup') {
showmessage('space_has_been_locked');
}
}
$actives = array($ac => ' class="a"');

list($seccodecheck, $secqaacheck) = seccheck('publish');

$navtitle = lang('core', 'title_setup');
if(lang('core', 'title_memcp_'.$ac)) {
```

```
$navtitle = lang('core', 'title_memcp_'.$ac);
}

$_G['disabledwidthauto'] = 0;

require_once libfile('spacecp/'.$ac, 'include');

?>
```

通过外部GET进来的ac参数指定了spacecp模块下的子模块为profile,最后进入include目录下的spacecp模块里面的接口文件spacecp_profile.php，这个文件即是

0x02 分析Discuz!X个人资料模块

通过上面的分析知道最终包含执行的文件是/source/include/spacecp/spacecp_profile.php 个人资料模块

第一部分，从数据库中读取出”个人资料”模块中的五个字段：”基本资料”、“联系方式”、“教育情况”、“工作情况”、“个人信息”，再提取出当前用户的原始个人信息：

```
if(!defined('IN_DISCUZ')) {
exit('Access Denied');
}
$defaultop = '';
$profilegroup = C::t('common_setting')->fetch('profilegroup', true);

foreach($profilegroup as $key => $value) {
if($value['available']) {
$defaultop = $key;
break;
}
}

$operation = in_array($_GET['op'], array('base', 'contact', 'edu', 'work', 'info', 'password', 'verify')) ? trim($_GET['op'])
$space = getuserbyuid($_G['uid']);
space_merge($space, 'field_home');
space_merge($space, 'profile');
```

从$operation里可见这个模块还包含了”密码安全的功能”(password)和"用户名修改”(verify)的字段

```
if(submitcheck('profilesubmit')) {

require_once libfile('function/discuzcode');

$forum = $setarr = $verifyarr = $errorarr = array();
$forumfield = array('customstatus', 'sightml');

$censor = discuz_censor::instance();

if($_GET['vid']) {
$vid = intval($_GET['vid']);
$verifyconfig = $_G['setting']['verify'][$vid];
if($verifyconfig['available'] && (empty($verifyconfig['groupid']) || in_array($_G['groupid'], $verifyconfig['groupid']))) {
$verifyinfo = C::t('common_member_verify_info')->fetch_by_uid_verifytype($_G['uid'], $vid);
if(!empty($verifyinfo)) {
$verifyinfo['field'] = dunserialize($verifyinfo['field']);
}
foreach($verifyconfig['field'] as $key => $field) {
if(!isset($verifyinfo['field'][$key])) {
$verifyinfo['field'][$key] = $key;
}
}
} else {
$_GET['vid'] = $vid = 0;
$verifyconfig = array();
}
}
if(isset($_POST['birthprovince'])) {
$initcity = array('birthprovince', 'birthcity', 'birthdist', 'birthcommunity');
foreach($initcity as $key) {
$_GET[''.$key] = $_POST[$key] = !empty($_POST[$key]) ? $_POST[$key] : '';
}
```

```
}
if(isset($_POST['resideprovince'])) {
$initcity = array('resideprovince', 'residecity', 'residedist', 'residecommunity');
foreach($initcity as $key) {
$_GET[''.$key] = $_POST[$key] = !empty($_POST[$key]) ? $_POST[$key] : '';
}
}
foreach($_POST as $key => $value) {

$field = $_G['cache']['profilesetting'][$key];

if(in_array($field['formtype'], array('text', 'textarea')) || in_array($key, $forumfield)) {

$censor->check($value);

if($censor->modbanned() || $censor->modmoderated()) {

profile_showerror($key, lang('spacecp', 'profile_censor'));

}

}


if(in_array($key, $forumfield)) {

if($key == 'sightml') {

loadcache(array('smilies', 'smileytypes'));

$value = cutstr($value, $_G['group']['maxsigsize'], '');

foreach($_G['cache']['smilies']['replacearray'] AS $skey => $smiley) {

$_G['cache']['smilies']['replacearray'][$skey] = '';

}

$value = preg_replace($_G['cache']['smilies']['searcharray'], $_G['cache']['smilies']['replacearray'], trim($value));
$forum[$key] = discuzcode($value, 1, 0, 0, 0, $_G['group']['allowsigbbcode'], $_G['group']['allowsigimgcode'], 0, 0, 1);
} elseif($key=='customstatus' && $allowcstatus) {
$forum[$key] = dhtmlspecialchars(trim($value));
}
continue;
} elseif($field && !$field['available']) {
continue;
} elseif($key == 'timeoffset') {
if($value >= -12 && $value <= 12 || $value == 9999) {
C::t('common_member')->update($_G['uid'], array('timeoffset' => intval($value)));
}
} elseif($key == 'site') {
if(!in_array(strtolower(substr($value, 0, 6)), array('http:/', 'https:', '[ftp://'](https://webmail.alibaba-inc.com/alimail/#t
$value = '[http://'.$value](http://%27.%24value/);
}
}
if($field['formtype'] == 'file') {
if((!empty($_FILES[$key]) && $_FILES[$key]['error'] == 0) || (!empty($space[$key]) && empty($_GET['deletefile'][$key]))) {
$value = '1';
} else {
$value = '';
}
}
if(empty($field)) {
continue;
} elseif(profile_check($key, $value, $space)) {
$setarr[$key] = dhtmlspecialchars(trim($value));
} else {
if($key=='birthprovince') {
$key = 'birthcity';
} elseif($key=='resideprovince' || $key=='residecommunity'||$key=='residedist') {
$key = 'residecity';
} elseif($key=='birthyear' || $key=='birthmonth') {
$key = 'birthday';
}
profile_showerror($key);
}
if($field['formtype'] == 'file') {
unset($setarr[$key]);
}
if($vid && $verifyconfig['available'] && isset($verifyconfig['field'][$key])) {
if(isset($verifyinfo['field'][$key]) && $setarr[$key] !== $space[$key]) {
$verifyarr[$key] = $setarr[$key];
}
unset($setarr[$key]);
}
if(isset($setarr[$key]) && $_G['cache']['profilesetting'][$key]['needverify']) {
if($setarr[$key] !== $space[$key]) {
$verifyarr[$key] = $setarr[$key];
}
unset($setarr[$key]);
}
}
if($_GET['deletefile'] && is_array($_GET['deletefile'])) {
foreach($_GET['deletefile'] as $key => $value) {
if(isset($_G['cache']['profilesetting'][$key])) {
@unlink(getglobal('setting/attachdir').'./profile/'.$space[$key]);
@unlink(getglobal('setting/attachdir').'./profile/'.$verifyinfo['field'][$key]);
$verifyarr[$key] = $setarr[$key] = '';
}
}
}
```

看到这里：

```
foreach($_POST as $key => $value):
```

其实这里可以联想到全局变量覆盖的问题，也就是通过这里来遍历外部的所有POST变量，然后将变量带入到下面的几处判断分支里面去，直到遍历完全部$_POST参数：

```
if(in_array($field['formtype'], array('text', 'textarea'))
if(in_array($key, $forumfield))
if($field['formtype'] == 'file’) //■■■■■■■■■■
if(empty($field)) //XSS■■
if($field['formtype'] == 'file’) //■■■■■■■■■■
if($vid && $verifyconfig['available'] && isset($verifyconfig['field'][$key]))
if(isset($setarr[$key]) && $_G['cache']['profilesetting'][$key]['needverify'])
```

变更数据信息通过变量覆盖原始数据传入数据库来达到更新数据的目的，下面的代码就是对上传文件的参数进行操作了：

```
if($_FILES) {
$upload = new discuz_upload();
foreach($_FILES as $key => $file) {
if(!isset($_G['cache']['profilesetting'][$key])) {
continue;
}
$field = $_G['cache']['profilesetting'][$key];
if((!empty($file) && $file['error'] == 0) || (!empty($space[$key]) && empty($_GET['deletefile'][$key]))) {
$value = '1';
} else {
$value = '';
}
if(!profile_check($key, $value, $space)) {
profile_showerror($key);
} elseif($field['size'] && $field['size']*1024 < $file['size']) {
profile_showerror($key, lang('spacecp', 'filesize_lessthan').$field['size'].'KB');
}
$upload->init($file, 'profile');
$attach = $upload->attach;

if(!$upload->error()) {
```

```
$upload->save();

if(!$upload->get_image_info($attach['target'])) {
@unlink($attach['target']);
continue;
}
$setarr[$key] = '';
$attach['attachment'] = dhtmlspecialchars(trim($attach['attachment']));
if($vid && $verifyconfig['available'] && isset($verifyconfig['field'][$key])) {
if(isset($verifyinfo['field'][$key])) {
@unlink(getglobal('setting/attachdir').'./profile/'.$verifyinfo['field'][$key]);
$verifyarr[$key] = $attach['attachment'];
}
continue;
}
if(isset($setarr[$key]) && $_G['cache']['profilesetting'][$key]['needverify']) {
@unlink(getglobal('setting/attachdir').'./profile/'.$verifyinfo['field'][$key]);
$verifyarr[$key] = $attach['attachment'];
continue;
}
@unlink(getglobal('setting/attachdir').'./profile/'.$space[$key]);
$setarr[$key] = $attach['attachment'];
}

}
}
```

这一块也是漏洞问题的触发点，详情在下面的漏洞分析中会分析，最终的SQL执行语句：

后面还有一个方法是password方法：

```
if($operation == 'password’) {
...
...
}
```

修改密码的模块，限于篇幅，不做过多的分析了。

0x03 漏洞分析

在说这个漏洞前，先说说14年Discuz的一个漏洞，也是任意文件操作漏洞，同样性质的漏洞，问题也是在spacecp_profile.php中出现的（毕竟新洞是继承了老洞的坑）

```
if($_GET['deletefile'] && is_array($_GET['deletefile'])) {
foreach($_GET['deletefile'] as $key => $value) {
if(isset($_G['cache']['profilesetting'][$key])) {
@unlink(getglobal('setting/attachdir').'./profile/'.$space[$key]);
@unlink(getglobal('setting/attachdir').'./profile/'.$verifyinfo['field'][$key]);
$verifyarr[$key] = $setarr[$key] = '';
}
}
}
```

首先判断外部是否有deletefile数组，然后对$_G[&#39;cache&#39;][&#39;profilesetting&#39;][$key]进行判断，看里面是否有值，这里比较关键的地方是:

```
>$_GET[&#39;deletefile&#39;] as $key =&gt; $value
```

这一步将外部指定的字段值给了$key值,比如外部是deletefile[affectivestatus]=1，那么$key值就是affectivestatus，

跟下去的$space[$key]就是数据库中个人资料的值(原始值)，带入到下面的unlink进行删除操作。

打印出来如下：

```
foreach($_GET['deletefile'] as $key => $value) {
if(isset($_G['cache']['profilesetting'][$key])) {
var_dump($_G['cache']['profilesetting'][$key]);

@unlink(getglobal('setting/attachdir').'./profile/'.$space[$key]);
var_dump($space[$key]);
exit();
```

后来官方出的补丁是：

```
if($_GET['deletefile'] && is_array($_GET['deletefile'])) {
foreach($_GET['deletefile'] as $key => $value) {
if(isset($_G['cache']['profilesetting'][$key]) && $_G['cache']['profilesetting'][$key]['formtype'] == 'file')
{
@unlink(getglobal('setting/attachdir').'./profile/'.$space[$key]);
@unlink(getglobal('setting/attachdir').'./profile/'.$verifyinfo['field'][$key]);
$verifyarr[$key] = $setarr[$key] = '';
}
}
}
```

直接加了类型(formtype)判断，只要判断出用户表单里面的类型为file后才走下一步，之前affectivestatus类型为text：

但是开发只修复了这一个点，同一个文件里面的其他unlink方法并没有Review到其中存在的安全威胁，导致了又一个任意文件删除漏洞：

```
if(!$upload->error()) {
$upload->save();

if(!$upload->get_image_info($attach['target'])) {
@unlink($attach['target']);
continue;
}
$setarr[$key] = '';
$attach['attachment'] = dhtmlspecialchars(trim($attach['attachment']));
if($vid && $verifyconfig['available'] && isset($verifyconfig['field'][$key])) {
if(isset($verifyinfo['field'][$key])) {
@unlink(getglobal('setting/attachdir').'./profile/'.$verifyinfo['field'][$key]);
$verifyarr[$key] = $attach['attachment'];
}
continue;
}
if(isset($setarr[$key]) && $_G['cache']['profilesetting'][$key]['needverify']) {
@unlink(getglobal('setting/attachdir').'./profile/'.$verifyinfo['field'][$key]);
$verifyarr[$key] = $attach['attachment'];
continue;
}
@unlink(getglobal('setting/attachdir').'./profile/'.$space[$key]);

$setarr[$key] = $attach['attachment'];
}
```

首先设置任意POST参数字段为你要删除的文件，然后再上传文件，网上很多是自己构造表单去上传文件，这里有个更简洁的方法，就是通过修改原始html表单的text参数为

保存截断跟踪参数走到
@unlink(getglobal(&#39;setting/attachdir&#39;).&#39;./profile/&#39;.$space[$key]);

debug参数如下：

同样还是获取到了affectivestatus的原始值参数并且拼接到unlink后面去造成了任意文件删除漏洞。

0x04 总结

最新的修复方案是官方直接把这个模块的所有unlink函数给删掉，简单又粗暴，不过确实真的有效办法，从这两次的重复出现的漏洞点可以看出，开发是值得反思的，这其

参考：

http://bobao.360.cn/learning/detail/4508.html
https://mp.weixin.qq.com/s/jZ4dh-Cseoe7i0ibNsANag
https://gitee.com/ComsenzDiscuz/DiscuzX/commit/7d603a197c2717ef1d7e9ba654cf72aa42d3e574

点击收藏 | 0 关注 | 1

上一篇：不重启Tomcat，覆盖本地代码 下一篇：NTP反射放大本地实验搭建遇到问题

1. 10 条回复

hades 2017-10-10 07:20:52

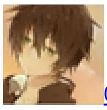
辛苦了 dz的代码太难读了~~

0 回复Ta

lenka 2017-10-10 07:30:07

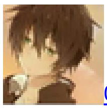
godiscuz域名到期了，尴尬

0 回复Ta

0r3ak 2017-10-10 07:37:31

确实到期了，那不妨搞一个dz架构安全分析专题

0 回复Ta

0r3ak 2017-10-10 07:39:04

毕竟是以前的老代码一次次迭代过来的，换用框架的话估计要花费太多的人力时间。

0 回复Ta

hades 2017-10-10 07:43:33

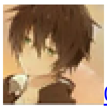
有兴趣的朋友可以联系我~   私信你

0 回复Ta

hades 2017-10-10 07:44:26

挖了这多年了~没有新技术产生 概率很小~

0 回复Ta

0r3ak 2017-10-10 07:48:01

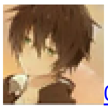
海贼师傅的随机数authkey安全问题，算是一个新思路吧。。。

0 回复Ta

xianzhi 2017-10-10 08:10:05

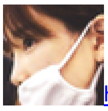
乍一看，还以为是这次的修复方式又被绕过了233

0 回复Ta

0r3ak 2017-10-10 08:14:42

额。。。unlink都被彻底干掉了，简单粗暴的方法，我的主题主要是借洞深入解析一下dz的结构，佩服你的Cobra，找时间看看，对企业级代码审计自动化很有帮助。

0 回复Ta

hades 2017-10-10 08:53:37

那把海贼的那个随机数authkey安全问题的文章发出来吧　最近php gd函数的利用也比较火~

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板