discuz任意文件删除漏洞的一点思考

具体的复现文章可参考：

https://paper.seebug.org/411/

```
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[$k
ey]) && empty($_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_lesstha
n').$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['at
tachment']));
                if($vid && $verifyconfig['available'] && isset($verifyconf
ig['field'][$key])) {
                    if(isset($verifyinfo['field'][$key])) {
                        @unlink(getglobal('setting/attachdir').'./profil
e/'.$verifyinfo['field'][$key]);
```

```
                        $verifyarr[$key] = $attach['attachment'];
                    }
                    continue;
                }
                if(isset($setarr[$key]) && $_G['cache']['profilesetting']
[$key]['needverify']) {
                    @unlink(getglobal('setting/attachdir').'./profile/'.$v
erifyinfo['field'][$key]);
                    $verifyarr[$key] = $attach['attachment'];
                    continue;
                }
                var_dump(getglobal('setting/attachdir').'./profile/'.$spac
e[$key]);
                @unlink(getglobal('setting/attachdir').'./profile/'.$space
[$key]);
                $setarr[$key] = $attach['attachment'];
            }

        }
    }
```

这里我说下我的一点思考，漏洞的定位点在修改个人配置里面的文件操作部分。
`spacecp_profile.php`的`if($_FILES)`分支。在这个分支里，会先上传图片（过程有检测），然后再判断验证信息，如果缺少对应的验证信息，则把之前上传的图片删除。这里的删除调用了`unlink`函数，这是一个根据传入路径删除文件的函数。

而文件的信息，经过`discuz_upload`类的初始化，会存储在其`attach`数组当中。对应的文件路径，则为`attach['target']`。因此，合理的做法是，无论是什么样的条件导致不能通过验证，都应该去调用：
`unlink($attach['target'])`

然而我们看到，在上述代码的最后一段，使用的是拼接变量`space[$key]`，`space`为用户个人配置的数组，`key`为上传文件中的`name`值，因此，只要修改个人配置信息为恶意变量，即可完成注入。

官方的修复方案是，直接把所有的`unlink`调用给删了..，可能他们自己也读不懂以前留下来的代码吧。

至于漏洞利用，大家可以发挥创造力，比如有人提出通过该漏洞删除安装锁，然后重装进后台再想办法getshell。