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:

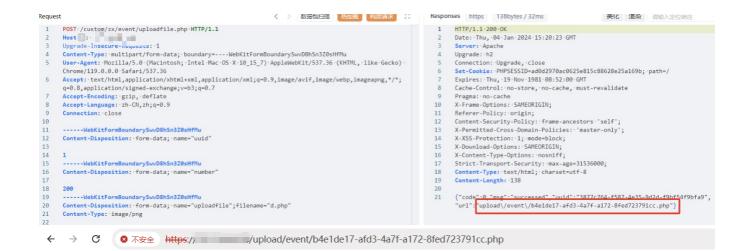
fofa语法:

FOFA: body="指挥调度管理平台"

漏洞复现:

payload:

效果图:



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_6
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/ghp-zts.d/dom.ini, /etc/php-zts.d/php-zts.d/ghp-zts.d/ghp-zts.d/ghp-zts.d/ghp-zts.d/ghp-zts.d/ghp-zts.d/php-zts.d/iconvzts.d/json.ini, /etc/php-zts.d/iconvzts.d/json.ini, /etc/php-zts.d/mbstring.ini, /etc/php-zts.d/mysqlnd.ini, /etc/php-zts.d/php-zts.d/php-zts.d/php-zts.d/php-zts.d/php-zts.d/php-zts.d/php-zts.d/php-zts.d/php-zts.d/php-zts.d/php-zts.d/shmop.ini, /etc/php-zts.d/chpp-zts.d/shmop.ini, /etc/php-zts.d/shmop.ini, /etc/php-zts.d/sh
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,TS
PHP Extension Build	API20170718,TS