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,可导致服务器失路。

网站图片:



网络测绘:

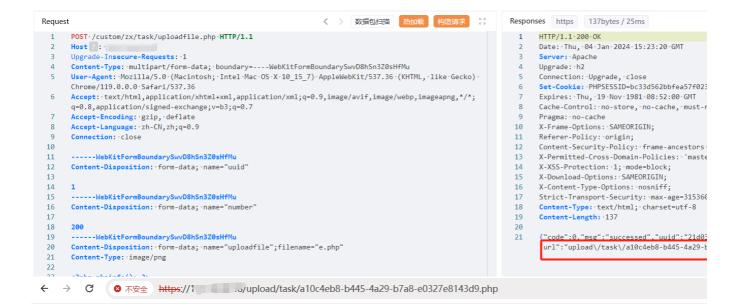
fofa语法:

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
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/gdr.ini, /etc/php-zts.d/gmp.ini, /etc/php-zts.d/icom zts.d/json.ini, /etc/php-zts.d/mbstring.ini, /etc/php-zts.d/mysqlnd.ini, /etc/php-zts /etc/php-zts.d/pocache.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/sdlite3.ini, /etc/php-zts.d/tokenizer.ini, /etc/php-zts.d/xml wddx.ini, /etc/php-zts.d/xmlwriter zts.d/xsl.ini, /etc/php-zts.d/zip.ini
PHP API	20170718
PHP Extension	20170718
7 15	220470740