New issue

smart-admin Druid application Unauthorized access #117

Open

y1shiny1shin opened 2 weeks ago

smart-admin Druid application Unauthorized access

NAME OF AFFECTED PRODUCT(S)

smart-admin

Vendor Homepage

- https://github.com/1024-lab/smart-admin

AFFECTED AND/OR FIXED VERSION(S)

submitter

- renyu

Vulnerable File

- /smart-admin-api/druid/index.html

VERSION(S)

- V3.30.0

PROBLEM TYPE

Vulnerability Type

- Unauthorized access

Root Cause

- In the "smart-admin" demo site,The developers failed to implement strict access control, allowing users to directly access the Druid page.

Impact

- Attackers can gain unauthorized access to all SQL statements and sessions in the system. After obtaining the session, they can log into the system backend and expand the damage.

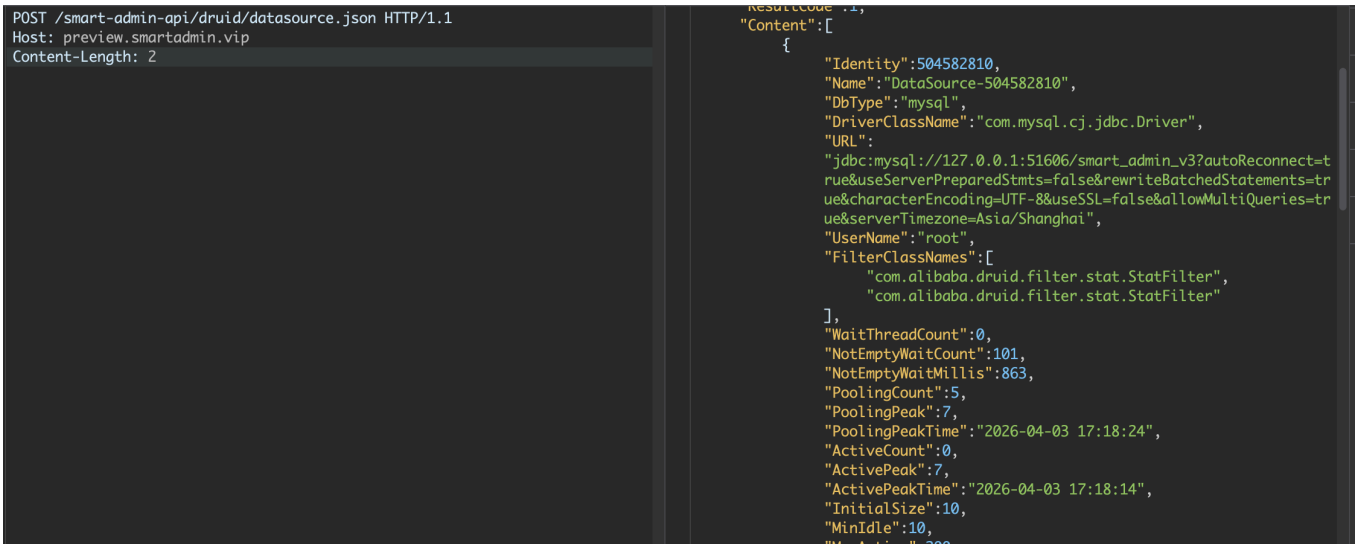
No login or authorization is required to exploit this vulnerability

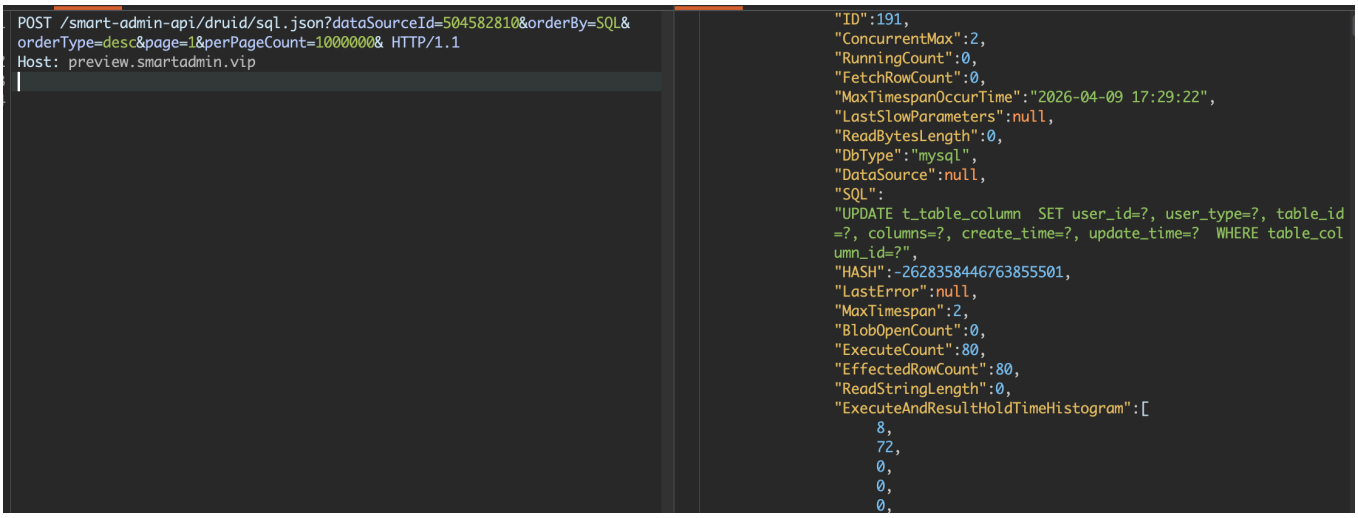
Vulnerability details and POC

Payload:

```
/smart-admin-api/druid/index.html
```

Details





Suggested repair

1. Add authentication to the Druid page and set a strong password.

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants