jeecgboot / **JeecgBoot** Public

Code Issues 22 Pull requests 13 Actions Projects Security and qua

⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

Commit b7c9aeb

jackieya committed 2 weeks ago

```
fix: add authentication check before loading sensitive AI tools in
sendWithDefault()

- Add user authentication check in sendWithDefault() before loading default tools
- Only authenticated users can access sensitive business tools (add_user, grant_user_roles,
etc.)
- Anonymous users can still use AI chat normally without sensitive tool access
- Fixes pre-auth AI chat tool abuse vulnerability
```

1 parent cf7eeac commit b7c9aeb

1 file changed +5 -1 lines changed

Top

Filter files…

jeecg-boot/jeecg-boot-module/jeecg-boot-module-airag/src/main/java/org/jeecg/modules/airag/app/serv…

AiragChatServiceImpl.java

1 file changed +5 -1 lines changed

Search within code

.../app/service/impl/AiragChatServiceImpl.java

```
@@ -1247,8 +1247,12 @@ private void sendWithDefault(String requestId,
ChatConversation chatConversation
1247  1247              aiChatParams = new AIChatParams();
1248  1248          }
1249  1249          // 如果是默认app,加载系统默认工具
```

```
                1250 +         // Security fix: 仅已登录用户可加载敏感业务工具(add_user,grant_user_roles
                     等),匿名用户仍可正常使用AI聊天
1250            1251
                     if(chatConversation.getApp().getId().equals(AiAppConsts.DEFAULT_APP_ID)){
1251            -              aiChatParams.setTools(jeecgToolsProvider.getDefaultTools());
                1252 +             String currentUser =
                     getUsername(SpringContextUtils.getHttpServletRequest());
                1253 +             if(oConvertUtils.isNotEmpty(currentUser)){
                1254 +                 aiChatParams.setTools(jeecgToolsProvider.getDefaultTools());
                1255 +             }
1252            1256             }
1253            1257             if(CollectionUtils.isEmpty(aiChatParams.getKnowIds())){
1254            1258                 aiChatParams.setKnowIds(chatConversation.getApp().getKnowIds());
```

Comments 0

Please sign in to comment.