

jeecgboot / JeecgBoot Public[Code](#) [Issues 22](#) [Pull requests 13](#) [Actions](#) [Projects](#) [Security and qua](#)

fix: add authentication check before loading sensitive AI tools in sendWithDefault() #9463



jackieya wants to merge 2 commits into jeecgboot:main from

jackieya:fix/airag-chat-tool-auth...



Conversation 5



Commits 2



Checks 0



Files changed 2



jackieya commented 2 weeks ago • edited ▾

Problem

The `sendWithDefault()` method in `AiragChatServiceImpl.java` unconditionally loads sensitive business tools (`add_user`, `query_user_by_name`, `query_all_roles`, `grant_user_roles`) for the default AI application, regardless of whether the current user is authenticated.

Since the `/airag/chat/send` endpoint is intentionally designed as a public endpoint (`@IgnoreAuth`), this allows unauthenticated attackers to invoke these sensitive tools through natural language instructions, potentially creating backdoor admin accounts and achieving full system takeover.

Root Cause

In `sendWithDefault()`, the code loads default tools without checking user authentication:

```
if(chatConversation.getApp().getId().equals(AiAppConsts.DEFAULT_APP_ID)){
    aiChatParams.setTools(jeecgToolsProvider.getDefaultTools());
    // No authentication check
}
```

Fix

Added `getUsername()` check before `setTools()`. Only authenticated users can now access sensitive business tools. Anonymous users can still use AI chat normally (preserving the `@IgnoreAuth` design intent).

```
if(chatConversation.getApp().getId().equals(AiAppConsts.DEFAULT_APP_ID)){
    String currentUser = getUsername(SpringContextUtils.getHttpServletRequest());
    if(oConvertUtils.isNotEmpty(currentUser)){
        aiChatParams.setTools(jeecgToolsProvider.getDefaultTools());
    }
}
```

Impact

- Sensitive tool loading is gated behind authentication

Follow-up Update: Enhance Fine-Grained Authorization for AI Assistant (Follow-up to PR [#9463](#))

Description

This PR supplements and strengthens the authorization logic introduced in PR [#9463](#) by addressing the lack of fine-grained permission control (vertical privilege escalation) within the AI Assistant module. The previous fix only verified whether a user was "logged in". This meant any authenticated low-privileged user (e.g., standard front-end user) could potentially utilize the AI Assistant to invoke or trigger sensitive backend tool execution like `add_user` or `grant_user_roles`, leading to unauthorized administrative actions and potential RCE.

Key Changes

This PR introduces robust, granular **runtime Shiro permission checks** to the core AI tool provider `JeecgBizToolsProvider.java`, achieving a perfect defense line with minimal code changes:

1. Dynamic ToolSpecification Pruning:

When registering and loading `getDefaultTools()` for the current LLM session, the system automatically validates whether the current logged-in user possesses the actual required backend business permissions (e.g., `system:user:add`) via `SecurityUtils.getSubject().isPermitted(...)`.

[fix: add authentication check before loading sensitive AI tools in se...](#) b7c9aeb



Copilot (AI) review requested due to automatic review settings [2 weeks ago](#)

Copilot [started reviewing](#) on behalf of **jackieya** [2 weeks ago](#)

[View session](#)

Copilot (AI) reviewed [2 weeks ago](#)

[View reviewed changes](#)

Copilot (AI) left a comment

Pull request overview

This PR hardens the public `/airag/chat/send` flow by preventing sensitive default business tools from being loaded in `sendWithDefault()` unless the caller is authenticated, aligning the default-chat behavior with the endpoint's `@IgnoreAuth` intent.

Changes:

- Gate `jeecgToolsProvider.getDefaultTools()` behind a `getUsername()` (authenticated user) check for the default AI app.
- Add an inline security comment clarifying why tool loading is conditional.

[Add Copilot custom instructions](#) for smarter, more guided reviews. [Learn how to get started.](#)



...odule-airag/src/main/java/org/jeecg/modules/airag/app/service/impl/AiragChatService
erviceImpl.java

Comment on lines +1250 to +1255

	1250	+	<code>// Security fix: 仅已登录用户可加载敏感业务工具(add_user, grant_user_</code>
1250	1251		<code>if(chatConversation.getApp().getId().equals(AiAppConsts.DEFAULT</code>
1251		-	<code>aiChatParams.setTools(jeecgToolsProvider.getDefaultTools())</code>
	1252	+	<code>String currentUser = getUsername(SpringContextUtils.getHttp</code>
	1253	+	<code>if(oConvertUtils.isEmpty(currentUser)){</code>
	1254	+	<code>aiChatParams.setTools(jeecgToolsProvider.getDefaultTool</code>
	1255	+	<code>}</code>

**Copilot** AI 2 weeks ago

当前仅用 `getUsername()` 判断“已登录”就加载默认工具，但

`jeecgToolsProvider.getDefaultTools()` (见 `JeecgBizToolsProvider`) 包含 `add_user / grant_user_roles` 等高权限操作，任何已登录普通用户仍可通过自然语言调用完成越权提权。建议在这里 (或在工具执行器内部) 增加更严格的授权校验 (例如仅管理员/具备特定权限的用户才注入这些工具)，或将默认工具拆分为“安全工具(所有登录用户)”与“管理工具(仅管理员)”两套。

[Copilot](#) uses AI. Check for mistakes.

**jackieya** 2 weeks ago

Author

关于权限粒度：本 PR 聚焦修复未认证用户 (Pre-auth) 可访问敏感工具的问题。已登录用户的角色级工具权限控制可以作为后续 PR 进一步加固。

```
...odule-airag/src/main/java/org/jeecg/modules/airag/app/service/impl/AiragChatsServiceImpl.java
```

Comment on lines 1251 to +1253

1250	1251		<code>if(chatConversation.getApp().getId().equals(AiAppConsts.DEFAULT_</code>
1251		-	<code>aiChatParams.setTools(jeecgToolsProvider.getDefaultTools())</code>
	1252	+	<code>String currentUser = getUsername(SpringContextUtils.getHttp</code>
	1253	+	<code>if(oConvertUtils.isEmpty(currentUser)){</code>

**Copilot** AI 2 weeks ago

这里的条件判断建议与同文件其它位置保持一致并避免潜在 NPE：使用

`AiAppConsts.DEFAULT_APP_ID.equals(chatConversation.getApp().getId())` (并统一 `if (/) {` 的空格风格)。这样即便后续 `appId` 为空也不会在 `equals` 处抛异常。

[Copilot](#) uses AI. Check for mistakes.

**jackieya** 2 weeks ago • edited ▾

Author

关于 NPE 风险：原始代码中统一使用了相同的写法，这里保持与原代码一致，减少 diff 范围，便于合并。

**jackieya** mentioned this pull request 2 weeks ago

Unauthenticated Sensitive Tool Loading in AI Chat Interface #9464

Closed



[fix\(airag\): add fine-grained shiro permission check for AI tools](#)

[2c1cc88](#)

[Sign up for free](#)

to join this conversation on **GitHub**. Already have an account? [Sign in to](#)

[comment](#)

Reviewers



Copilot



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants

