

fix(backend/ws): Add user_id to websocket event subscription key #9660

New issue

Merged

Pwuts merged 6 commits into master from pwuts/secr1-1194-prevent-users-from-receiving-each-others-graph-execution last month


Conversation 8

Commits 6

Checks 17


Files changed 6

+198 -49

 Pwuts commented last month • edited


Member


- Add user_id to WS subscription key
- Add error catching to WS message handler


 fix(backend/ws): Filter websocket execution events by user ID

Verified

3989003


 Pwuts requested a review from a team as a code owner last month


 Pwuts requested review from kcze and aarushik93 and removed request for a team last month

 github-project-automation bot moved this to


NEW


 Needs initial review in AutoGPT development kanban last month


 github-project-automation bot added this to AutoGPT development kanban last month

 supabase bot commented last month

Reviewers

 Bentlybro

 kcze

 aarushik93


Assignees

No one assigned

Labels

platform/backend Security size/l

Projects

 AutoGPT development kan...

▼

Status:

✓

 Done +2 more

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants

This pull request has been ignored for the connected project `bgwpwdsxblryihinutbx` because there are no changes detected in `supabase` directory. You can change this behaviour in [Project Integrations Settings ↗](#).

Preview Branches by Supabase.

Learn more about [Supabase Branching ↗](#).



github-actions bot commented last month

Contributor

This PR targets the `master` branch but does not come from `dev` or a `hotfix/*` branch.

Automatically setting the base branch to `dev`.



github-actions bot changed the base branch from `master` to `dev` last month



qodo-merge-pro bot added the `Review effort 3/5` label last month



qodo-merge-pro bot commented last month

Qodo Merge was enabled for this repository. To continue using it, please link your Git account with your Qodo account [here](#).

PR Reviewer Guide 🔍

Here are some key observations to aid the review process:

Estimated effort to review: 3

PR contains tests

No security concerns identified

Recommended focus areas for review

► [Access Control](#)

The implementation adds user ID verification for graph access, but there's no error handling if `get_db_client().get_graph()` fails for reasons other than access control (e.g., database connection issues).

► [Error Handling](#)

The `from_db` method now requires either a `graph_execution` with `userId` or an explicit `user_id` parameter. If both are missing, it raises a `ValueError`, but callers might not be prepared to handle this exception.



github-actions

(bot)

added platform/backend size/l

and removed Review effort 3/5 labels last month





netlify

(bot)

commented last month • edited ▾



Deploy Preview for *auto-gpt-docs* canceled.

Name	Link
 Latest commit	f99df96
 Latest deploy log	https://app.netlify.com/sites/auto-gpt-docs/deloys/67dc412276da950008671c88



deepsource-io







(bot)

commented last month • edited ▾

Here's the code health analysis summary for commits

90b147f...f99df96 . [View details on DeepSource](#) ↗.

Analysis Summary

Analyzer	Status	Summary	Link
 JavaScript	 Success		View Check ↗
 Python	 Success	 4 occurrences introduced  3 occurrences resolved	View Check ↗

💡 If you're a repository administrator, you can configure the quality gates from the [settings](#).

🔗  format



Verified

✗ a71fffd




netlify bot commented last month • edited ▾


✅ **Deploy Preview for *auto-gpt-docs-dev* canceled.**


Name	Link
 Latest commit	f99df96
 Latest deploy log	https://app.netlify.com/sites/auto-gpt-docs-dev/deployments/67dc4122e1b72600081fd0f7

🔗 **Pwuts** added 4 commits [last month](#)

🔗  add error handling for websocket endpoints Verified ✗ ef8ba77

🔗  fix tests (partially) Verified ✓ 0fd26ec

🔗  disable broken and redundant access check Verified ✗ e88b50a

🔗  fix test Verified ✓ f99df96



👁 **Bentlybro** reviewed last month [View reviewed changes](#)



autogpt_platform/backend/backend/
server/ws_api.py


⚙ Show resolved


🔗  **Pwuts** enabled auto-merge last month




👁 **Bentlybro** previously approved these changes last month [View reviewed changes](#)

 **github-project-automation** bot moved this from NEW
Needs initial review to  **Mergeable** in **AutoGPT**
development kanban last month


 **Pwuts** added this pull request to the merge queue
last month

 **Pwuts** removed this pull request from the
merge queue due to a manual request [View details](#)
last month


 **Pwuts** changed the base branch from `dev` to `master`
last month




× **Pwuts** dismissed **Bentlybro**'s stale review last month

The base branch was changed.

 **Pwuts** changed the title ~~**fix(backend/ws): Filter**~~
~~**websocket execution events by user ID**~~ **fix(backend/ws):**
Add `user_id` to websocket event subscription key
last month

Pwuts merged commit **9a661b5** into
`master` last month
24 checks passed [View details](#)

 **Pwuts** deleted the
`pwuts/secret-1194-prevent-users-from-receiving-each-ot...`
branch last month

 **github-project-automation** bot moved this from 
Mergeable to  **Done** in **AutoGPT** **development kanban**
last month

 **Pwuts** added the `Security`  label last month