Cross-user sharing of node execution results through WebSockets API

Low **ntindle** published **GHSA-958f-37vw-jx8f** 4 days ago

Package	Affected versions	Patched versions
autogpt-platform-backend	< 0.6.1	0.6.1

Description

Impact

The AutoGPT Platform's WebSocket API transmitted node execution updates to subscribers based on the `graph_id` + `graph_version`. Additionally, there was no check prohibiting users from subscribing with another user's `graph_id` + `graph_version`.

As a result, node execution updates from one user's graph execution could be received by another user within the same instance in either of two scenarios:

- Through the Marketplace, multiple users have access to the same graph. If their clients are active and subscribed to an execution simultaneously, they could have received node execution updates from each other.
- A malicious actor acquires a `graph_id` and `graph_version` belonging to another user (their target) and subscribes to the target user's graph executions directly through the WS API.

This vulnerability *does not* occur between different instances or between users and non-users of the platform. Single-user instances are not affected. In private instances with a user white-list, the impact is limited by the fact that all potential unintended recipients of these node execution updates must have been admitted by the administrator.

Patches

The problem was patched - and the patch rolled out to production - the day of discovery:
fix(backend/ws): Add `user_id` to websocket event subscription key - #9660

Severity

Low 3.5 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N

CVE ID

CVE-2025-31494

Weaknesses

CWE-200 CWE-284

Credits

 **Pwuts** Finder

The patch was also included in the subsequent release of the platform: AutoGPT Platform v0.6.1

We discovered this vulnerability ourselves, and have no indication whether anyone else found or experienced this vulnerability up until we found it.