Unauthenticated SSE Event Stream Exposes All Agent Activity in A2U Server

High **MervinPraison** published **GHSA-f292-66h9-fpmf** yesterday

Package

praisonai (pip)

Affected versions	Patched versions
<= 4.5.114	>= 4.5.115

Description

The A2U (Agent-to-User) event stream server in PraisonAI exposes all agent activity without authentication. This is a separate component from the gateway server fixed in CVE-2026-34952.

The create_a2u_routes() function registers the following endpoints with NO authentication checks:

- GET /a2u/info — exposes server info and stream names
- POST /a2u/subscribe — creates event stream subscription
- GET /a2u/events/{stream_name} — streams ALL agent events
- GET /a2u/events/sub/{id} — streams events for subscription
- GET /a2u/health — health check

An unauthenticated attacker can:

1. POST /a2u/subscribe → receive subscription_id
2. GET /a2u/events/sub/{subscription_id} → receive live SSE stream of all agent events including responses, tool calls, and thinking

This exposes sensitive agent activity including responses, internal reasoning, and tool call arguments to any network attacker.

```
(base) srisowmyanemani@Srisowmyas-MacBook-Pro PraisonAI % >....
import ast, sys

# Read the source file directly
with open('src/praisonai/praisonai/endpoints/a2u_server.py', 'r') as f:
    source = f.read()

# Confirm no auth in a2u_info
has_auth_check = '_check_auth' in source or 'auth_token' in source or 'Authorization' in source
no_auth_routes = 'a2u_info' in source and 'a2u_subscribe' in source

print('=== A2U Auth Analysis ===')
print(f'Auth check present in a2u_server.py: {has_auth_check}')
print(f'Unauthenticated routes present: {no_auth_routes}')
print(f'Vulnerable: {not has_auth_check and no_auth_routes}')

# Show the exact vulnerable function
lines = source.split('\n')
for i, line in enumerate(lines):
    if 'async def a2u_subscribe' in line or 'async def a2u_events' in line or 'async def a2u_info' in line
:
        print(f'Line {i+1}: {line.strip()} -- NO auth check')
"
=== A2U Auth Analysis ===
Auth check present in a2u_server.py: False
Unauthenticated routes present: True
Vulnerable: True
Line 243: async def a2u_info(request): -- NO auth check
Line 259: async def a2u_subscribe(request): -- NO auth check
Line 296: async def a2u_events_stream(request): -- NO auth check
Line 320: async def a2u_events_subscription(request): -- NO auth check
(base) srisowmyanemani@Srisowmyas-MacBook-Pro PraisonAI %
```

```
=== PraisonAI A2U Unauthenticated Access PoC ===

[1] POST /a2u/subscribe (no auth token)
    Status: 200
    Response: {"subscription_id":"sub-a1ad8a6edd8b","stream_name":"events","stream_url":"http://testserver
/a2u/events/sub-a1ad8a6edd8b","created_at":"2026-04-07T01:44:15.102943+00:00"}
    Got subscription_id: sub-a1ad8a6edd8b

[2] GET /a2u/info (no auth token)
    Status: 200
    Response: {"name":"A2U Event Stream","version":"1.0.0","streams":["events"],"event_types":["agent.star
ted","agent.thinking","agent.tool_call","agent.response","agent.completed","agent.error"]}

[3] GET /a2u/health (no auth token)
    Status: 200
    Response: {"status":"healthy","active_subscriptions":1,"active_streams":1}

VULNERABLE: All endpoints accessible without any authentication
Impact: Attacker can subscribe and receive ALL agent events including
        responses, tool calls, and internal reasoning in real-time
```

[1] POST /a2u/subscribe (no auth token)
Status: 200
Response: {"subscription_id":"sub-a1ad8a6edd8b","stream_name":"events",
"stream_url":"http://testserver/a2u/events/sub-a1ad8a6edd8b"}
Got subscription_id: sub-a1ad8a6edd8b

[2] GET /a2u/info (no auth token)
Status: 200
Response: {"name":"A2U Event Stream","version":"1.0.0",
"streams":["events"],"event_types":["agent.started","agent.thinking",
"agent.tool_call","agent.response","agent.completed","agent.error"]}

[3] GET /a2u/health (no auth token)
Status: 200
Response: {"status":"healthy","active_subscriptions":1,"active_streams":1}

Impact: Attacker can subscribe and receive ALL agent events including responses, tool calls, and internal reasoning in real-time

Severity

High 7.5 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-39889

Weaknesses

No CWEs

Credits

 **srisowmya2000** Reporter