Improper Mass Assignment in Account Registration Enables Unauthorized Organization Association

High **igor-magun-wd** published **GHSA-48m6-ch88-55mj** last week

Package

flowise (npm)

Affected versions

<= 3.0.13

Patched versions

3.1.0

Description

Summary

An improper mass assignment (JSON injection) vulnerability in the account registration endpoint of Flowise Cloud allows unauthenticated attackers to inject server-managed fields and nested objects during account creation. This enables client-controlled manipulation of ownership metadata, timestamps, organization association, and role mappings, breaking trust boundaries in a multi-tenant environment.

Details

The POST /api/v1/account/register endpoint is intended to accept a minimal payload to create a new user account (e.g., name, email, password). However, the backend fails to enforce a strict allowlist or DTO-based validation and instead blindly maps client-supplied JSON to internal domain models.

As a result, attackers can include additional nested objects and server-managed fields in the request body such as organization, organizationUser, workspace, workspaceUser, and metadata fields like createdBy, updatedBy, createdDate, and updatedDate. These fields are persisted as provided by the client rather than being generated or validated server-side.

This behavior demonstrates a trust boundary violation where authorization and ownership decisions that must be enforced by the server are effectively delegated to untrusted client input. In a multi-tenant SaaS context, this can lead to unauthorized organization association and role assignment during registration.

PoC

Send a standard registration request:

```
POST /api/v1/account/register HTTP/2
Host: cloud.flowiseai.com
Content-Type: application/json

{
  "user": {
    "name": "Test User",
    "email": "testuser@example.com",
    "credential": "StrongPassword123!"
  }
}
```

Observe the 201 Created response returning a newly created user and related objects (organization, workspace, roles).

Send a modified registration request that injects additional server-managed fields and nested objects:

POST /api/v1/account/register HTTP/2
Host: cloud.flowiseai.com
Content-Type: application/json

```
{
  "user": {
    "name": "Injected User",
    "email": "injected@example.com",
    "credential": "StrongPassword123!",
    "createdBy": "<arbitrary-uuid>",
    "updatedBy": "<arbitrary-uuid>",
    "createdDate": "1999-12-27T13:10:47.666Z",
    "updatedDate": "1999-12-27T13:10:47.666Z"
  },
  "organization": {
    "id": "<existing-organization-uuid>",
    "name": "Injected Organization"
  },
  "organizationUser": {
    "organizationId": "<existing-organization-uuid>",
    "roleId": "<owner-role-uuid>"
  }
}
```

Observe that the server responds with 201 Created and persists the injected fields, reflecting client-controlled values for ownership metadata, timestamps, and organization association.

Impact

- Vulnerability Class: Mass Assignment / JSON Injection / Improper Input Validation.
- Who is impacted: All deployments of Flowise Cloud exposing the registration endpoint.

By supplying a known organizationId during registration, an unauthenticated attacker can create a new user account directly associated with an existing organization they do not belong to. This results in unauthorized cross-tenant access and privilege escalation at account creation time, completely bypassing organizational ownership and trust boundaries.

Security Consequences:

1. Client-controlled manipulation of server-managed fields (audit timestamps, ownership metadata).
2. Unauthorized association of newly created accounts with existing organizations.
3. Injection of role and membership relationships during registration.
4. Violation of trust boundaries in a multi-tenant environment, increasing the risk of privilege abuse and audit integrity failures.

Severity

High 8.1 / 10

CVSS v3 base metrics

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

Learn more about base metrics

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2026-41267

Weaknesses

- CWE-20
- CWE-639
- CWE-915

Credits

berkdedekarginoglu Reporter