

**GOVERNMENT OF THE REPUBLIC  
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU  
DEPARTMENT OF COMMUNICATIONS  
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOUVERNEMENT DE LA  
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE  
COMMUNICATION ET DE  
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

11 September 2026

**Advisory 299: Flowise Prediction Endpoint Unauthenticated Remote Code Execution - No Vendor Patch Available (CVE-2026-52098).**

**Release Date:** 10<sup>th</sup> September 2026

**Impact:** **CRITICAL**

**TLP:** CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and developers that operate a self-hosted Flowise instance for building or running visual, low-code AI agent and LLM application workflows. This alert is intended to be understood by technical users and systems administrators.

## What is it?

CVE-2026-52098 is a critical, unauthenticated remote code execution vulnerability in Flowise, a widely-adopted open-source, low-code visual builder for AI agents and LLM applications (over 55,000 GitHub stars at the time of writing). A remote attacker can execute arbitrary code via the "/api/v1/prediction/<flowId>" endpoint, without requiring authentication.

## What are the systems affected?

The following version(s) are affected:

- Flowise (FlowiseAI/Flowise), version 3.1.2 and, given the project's archived status, presumed all subsequent and prior versions relying on the same prediction endpoint - (Affected)

# What does this mean?

## Typical attack flow:

1. **Reach the Flowise prediction endpoint with a crafted request**
  - A remote, unauthenticated attacker sends a specially crafted request to a reachable Flowise instance's `/api/v1/prediction/<flowId>` endpoint.
2. **Achieve arbitrary code execution**
  - The crafted request triggers code injection in the prediction-handling logic, allowing the attacker to execute arbitrary code on the server hosting the Flowise instance, without any authentication.

## Attack vectors:

- A network-based, unauthenticated attack against any Flowise instance with its prediction API reachable from an untrusted network, most critically the public internet.

Successful exploitation may allow attackers to:

- Execute arbitrary code on the server hosting the Flowise instance, without any authentication.
- Use that code execution to access any credentials, connected data sources, or downstream systems the Flowise instance's AI workflows are configured to use, and potentially pivot into the wider network hosting it.

# Mitigation process

CERTVU recommends the following:

1. Restrict network access to the Flowise instance
  - Since no vendor patch exists or is expected, restrict access to the Flowise prediction API to trusted internal networks only, and ensure it is never directly reachable from the internet.
2. Place the instance behind a Web Application Firewall (WAF)
3. Evaluate migrating to an actively-maintained alternative
4. Monitor for unauthorized activity on the platform

Report any suspected compromise of a Flowise deployment to CERTVU at [incident@cert.gov.vu](mailto:incident@cert.gov.vu) or on telephone (678) 33380.

# Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-52098>
2. <https://github.com/FlowiseAI/Flowise>