



# AgentFlow Local Web API Content-Type Validation Bypass

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-7439
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-29 19:16:26 UTC
<b>Updated</b>	2026-04-30 15:44:48 UTC
<b>Description</b>	AgentFlow's local web API accepts non-JSON content types on POST /api/runs and POST /api/runs/validate endpoints with

## Risk And Classification

**Primary CVSS:** v4.0 4.8 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000060000 probability, percentile 0.004190000 (date 2026-05-05)

**Problem Types:** CWE-346 | CWE-346 CWE-346: Origin Validation Error

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA
4.0	CNA	CVSS	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA
3.1	disclosure@vulncheck.com	Secondary	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Berabuddies	AgentFlow	affected 1667fa3 git	Not specified

### References

Reference	Source	Link
github.com/berabuddies/agentflow/commit/1667fa3	disclosure@vulncheck.com	github.com
www.vulncheck.com/advisories/agentflow-local-web-api-content-type-validation-by...	disclosure@vulncheck.com	www.vulnc
github.com/berabuddies/agentflow/pull/18	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Chia Min Jun Lennon (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)