



# FastGPT: DNS rebinding TOCTOU bypass in isInternalAddress allows SSRF on all protected endpoints

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

## Summary

<b>CVE</b>	CVE-2026-42344
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-08 23:16:37 UTC
<b>Updated</b>	2026-05-08 23:16:37 UTC
<b>Description</b>	FastGPT is an AI Agent building platform. In versions 4.14.11 and prior, FastGPT's isInternalAddress() function in package:

## Risk And Classification

**Primary CVSS:** v3.1 6.3 MEDIUM from security-advisories@github.com

**CVSS:** 3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

**Problem Types:** CWE-367 | CWE-367 CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
3.1	CNA	DECLARED	6.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**High**

Privileges Required

**Low**

User Interaction

**None**

Scope

**Changed**

Confidentiality

High

Integrity

None

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Labring	FastGPT	affected <= 4.14.11	Not specified

### References

Reference	Source	Link	Tags
github.com/labring/FastGPT/security/advisories/GHSA-cc8x-jrqv-hmwh	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)