



FastGPT: Stored MCP tool URL SSRF in FastGPT workflow execution

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

Summary

CVE	CVE-2026-44284
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 23:16:39 UTC
Updated	2026-05-08 23:16:39 UTC
Description	FastGPT is an AI Agent building platform. Prior to version 4.14.17, FastGPT had an inconsistent SSRF protection gap in M

Risk And Classification

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

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

Problem Types: CWE-918 | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Labring	FastGPT	affected < 4.14.17	Not specified

References

Reference	Source	Link	Te
github.com/labring/FastGPT/pull/6826	security-advisories@github.com	github.com	
github.com/labring/FastGPT/commit/c1c6b9520d976d25ed945b5bc4e0768149e6db69	security-advisories@github.com	github.com	
github.com/labring/FastGPT/releases/tag/v4.14.17	security-advisories@github.com	github.com	
github.com/labring/FastGPT/security/advisories/GHSA-cxxj-99f7-f5wq	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

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](#)

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