



# Server-Side Request Forgery via MCP Tools Endpoint in FastGPT

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

## Summary

<b>CVE</b>	CVE-2026-34163
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 15:16:17 UTC
<b>Updated</b>	2026-04-01 18:28:47 UTC
<b>Description</b>	FastGPT is an AI Agent building platform. Prior to version 4.14.9.5, FastGPT's MCP (Model Context Protocol) tools endpoint

## Risk And Classification

**Primary CVSS:** v3.1 7.7 HIGH from nvd@nist.gov

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

**EPSS:** 0.000280000 probability, percentile 0.077360000 (date 2026-04-01)

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.7	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
3.1	security-advisories@github.com	Secondary	7.7	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
3.1	CNA	DECLARED	7.7	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fastgpt	Fastgpt	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Labring	FastGPT	affected < 4.14.9.5	Not specified

### References

Reference	Source	Link	Tags
github.com/labring/FastGPT/pull/6640	security-advisories@github.com	github.com	Issue
github.com/labring/FastGPT/releases/tag/v4.14.9.5	security-advisories@github.com	github.com	Product
github.com/labring/FastGPT/security/advisories/GHSA-x9vj-5m4j-9mfv	security-advisories@github.com	github.com	Exploit
github.com/labring/FastGPT/commit/bc7eae2ed61481a5e322208829be291faec58c00	security-advisories@github.com	github.com	Package
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

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.

CVE.report and Source URL Uptime Status status.cve.report