Server-Side Request Forgery via MCP Tools Endpoint in FastGPT

MITRE | NVD | CVE.ORG | Print: PDF

Summary

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

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

ntegrity

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	Ta
github.com/labring/FastGPT/pull/6640	security-advisories@github.com	github.com	Iss
github.com/labring/FastGPT/releases/tag/v4.14.9.5	security-advisories@github.com	github.com	Pro
github.com/labring/FastGPT/security/advisories/GHSA-x9vj-5m4j-9mfv	security-advisories@github.com	github.com	Ex
github.com/labring/FastGPT/commit/bc7eae2ed61481a5e322208829be291faec58c00	security-advisories@github.com	github.com	Pa
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.