vLLM affected by Server-Side Request Forgery (SSRF) in `download_bytes_from_url `

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-34753
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-06 16:16:36 UTC
Updated	2026-04-07 13:20:11 UTC
Description	vLLM is an inference and serving engine for large language models (LLMs). From 0.16.0 to before 0.19.0, a server-side req

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from security-advisories@github.com

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

EPSS: 0.000340000 probability, percentile 0.098100000 (date 2026-04-07)

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	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Vllm-project	Vllm	affected >= 0.16.0, < 0.19.0	Not specified

References

Reference	Source	Link	Tags
github.com/vllm-project/vllm/security/advisories/GHSA-pf3h-qjgv-vcpr	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.