VDB-355283 · CVE-2026-5530 · GCVE-100-355283

OLLAMA UP TO 18.1 MODEL PULL API SERVER/DOWNLOAD.GO SERVER-SIDE REQUEST FORGERY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
6.1	$0-$5k	1.68-

Summary

A vulnerability was found in Ollama up to 18.1. It has been classified as critical. Impacted is an unknown function of the file *server/download.go* of the component *Model Pull API*. The manipulation leads to server-side request forgery. This vulnerability is listed as CVE-2026-5530. The attack may be initiated remotely. There is no available exploit. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability was found in Ollama up to 18.1. It has been rated as critical. This issue affects an unknown code block of the file *server/download.go* of the component *Model Pull API*. The manipulation with an unknown input leads to a server-side request forgery vulnerability. Using CWE to declare the problem leads to CWE-918. The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination. Impacted is confidentiality, integrity, and availability.

The identification of this vulnerability is CVE-2026-5530. The exploitation is known to be easy. The attack may be initiated remotely. Technical details of the vulnerability are known, but there is no available exploit. The pricing for an exploit might be around USD $0-$5k at the moment (estimation calculated on 04/04/2026).

The vendor was contacted early about this disclosure but did not respond in any way.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

See VDB-300376, VDB-300378, VDB-300379 and VDB-300394 for similar entries.

Product

Name

- Ollama

Version

- 18.0
- 18.1

CPE 2.3

- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 6.1

VulDB Base Score: 6.3
VulDB Temp Score: 6.1
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Server-side request forgery
CWE: CWE-918
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Status: Not defined
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/04/2026		Advisory disclosed
04/04/2026	+0 days	VulDB entry created
04/04/2026	+0 days	VulDB entry last update

Sources

Status: Not defined

CVE: CVE-2026-5530 (🔒)
GCVE (CVE): GCVE-0-2026-5530
GCVE (VulDB): GCVE-100-355283
See also: 🔒

Entry

Created: 04/04/2026 08:34 AM
Changes: 04/04/2026 08:34 AM (51)
Complete: 🔍
Submitter: davidrochester
Cache ID: 172:7B3:179

Submit

Accepted

- Submit #782107: Ollama 18.1 and previous Server-Side Request Forgery (by davidrochester)

Discussion

No comments yet. Languages: en.

Please log in to comment.