VDB-355285 · CVE-2026-5532 · GCVE-100-355285

SCRAPEGRAPHAI SCRAPEGRAPH-AI UP TO 1.74.0 GENERATECODENODE GENERATE_CODE_NODE.PY CREATE_SANDBOX_AND_EXECUTE OS COMMAND INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	3.13-

Summary

A vulnerability was found in ScrapeGraphAI scrapegraph-ai up to 1.74.0. It has been rated as critical. The impacted element is the function `create_sandbox_and_execute` of the file *scrapegraphai/nodes/generate_code_node.py* of the component *GenerateCodeNode Component*. This manipulation causes os command injection. This vulnerability is registered as CVE-2026-5532. Remote exploitation of the attack is possible. Furthermore, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability classified as critical was found in ScrapeGraphAI scrapegraph-ai up to 1.74.0. Affected by this vulnerability is the function `create_sandbox_and_execute` of the file *scrapegraphai/nodes/generate_code_node.py* of the component *GenerateCodeNode Component*. The manipulation with an unknown input leads to a os command injection vulnerability. The CWE definition for the vulnerability is CWE-78. The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared at github.com. This vulnerability is known as CVE-2026-5532. The exploitation appears to be easy. The attack can be launched remotely. The exploitation doesn't need any form of authentication. It demands that the victim is doing some kind of user interaction. Technical details and also a public exploit are known. MITRE ATT&CK project uses the attack technique T1202 for this issue.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. 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.

Product

Type

- Artificial Intelligence Software

Vendor

- ScrapeGraphAI

Name

- scrapegraph-ai

Version

- 1.0
- 1.1
- 1.2
- 1.3
- 1.4
- 1.5
- 1.6
- 1.7
- 1.8
- 1.9
- 1.10
- 1.11
- 1.12
- 1.13

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Os command injection
CWE: CWE-78 / CWE-77 / CWE-74
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public

Status: Proof-of-Concept
Download: 🔒
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

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5532 (🔒)
GCVE (CVE): GCVE-0-2026-5532
GCVE (VulDB): GCVE-100-355285
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/04/2026 08:38 AM
Changes: 04/04/2026 08:38 AM (58)
Complete: 🔍

Submitter: Yu Bao
Cache ID: 20:EC3:179

Submit

Accepted

- Submit #782169: ScrapeGraphAI scrapegraph-ai 1.74.0 Remote Code Execution (RCE) (by Yu Bao)

Discussion

No comments yet. Languages: en.

Please log in to comment.