Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-3248: Langflow AI Workflow Platform RCE

Date of Publication	Admiralty Code	TA Number
May 6, 2025	A1	TA2025137

Summary

First Seen: February 22, 2025
Affected Product: Langflow
Impact: CVE-2025-3248 is a critical RCE vulnerability in Langflow <1.3.0, caused by unsafe use of Python’s exec() in the /api/v1/validate/code endpoint, allowing unauthenticated attackers to execute arbitrary code via decorators or default arguments. This can lead to full system compromise without authentication. Public PoCs exist, and active exploitation has been observed. Upgrade to Langflow 1.3.0 or restrict endpoint access immediately to mitigate this severe threat.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-3248	Langflow Missing Authentication Vulnerability	Langflow	✗	✓	✓

Vulnerability Details

#1

CVE-2025-3248 is a critical remote code execution (RCE) vulnerability affecting Langflow versions prior to 1.3.0. Langflow is an open-source tool (58K+ GitHub stars) for building AI-driven agents via a visual web interface. The flaw lies in the /api/v1/validate/code endpoint, which improperly uses Python's exec() function on user-supplied code without sufficient input validation or authentication. This allows unauthenticated attackers to inject and execute arbitrary Python code on the server, leading to full system compromise without requiring any credentials.

#2

The vulnerability arises because Langflow parses and processes user-submitted code by compiling it into an Abstract Syntax Tree (AST), during which Python decorators and default argument values are evaluated immediately. Attackers exploit this behavior by embedding malicious payloads in these constructs, which execute as soon as the code is processed. Since the endpoint lacks proper authentication and sandboxing, it is highly susceptible to remote exploitation.

#3

The vulnerability has a CVSS score of 9.8, reflecting its critical severity and ease of exploitation. The potential impact is severe: successful exploitation gives attackers full access to the underlying operating system, enabling them to read sensitive files, exfiltrate data, deploy malware, or move laterally within a network. Confirmed exploitation attempts have already been observed in the wild, including scans from TOR nodes and payloads attempting to read system files like /etc/passwd.

#4

Nearly 500 Langflow instances exposed on the internet remain vulnerable, posing significant risks to organizations using the tool for AI workflow development. This incident underscores the critical need for secure coding practices, particularly around input validation and authentication, in AI development platforms that execute user-supplied code.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-3248	Langflow versions prior to 1.3.0	cpe:2.3:a:langflow-ai:langflow:*:*:*:*:*:*:*:*	CWE-306

Recommendations

Upgrade Langflow: Immediately update to Langflow version 1.3.0 or later, where the vulnerability has been patched. This is the most effective and recommended fix.

Restrict Endpoint Access: Ensure the /api/v1/validate/code endpoint is not exposed to the internet. Limit access using firewalls, reverse proxies, or VPNs.

Enforce Authentication: If updating isn't immediately possible, implement authentication controls at the network or application level to restrict access to the validation endpoint.

Monitor for Exploitation Attempts: Watch for unusual POST requests to the /validate/code endpoint or signs of subprocess execution (e.g., os.system, subprocess usage) in logs. Implement alerting for known exploit patterns.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**T1588** Obtain Capabilities	**T1588.005** Exploits	**T1059.006** Python
T1204.002 Malicious File	**T1190** Exploit Public-Facing Application	**T1204** User Execution	**T1588.006** Vulnerabilities

Patch Details

Upgrade to Langflow 1.3.0 or later versions.

Link:
https://github.com/langflow-ai/langflow/releases/tag/1.3.0

References

https://www.zscaler.com/blogs/security-research/cve-2025-3248-rce-vulnerability-langflow

https://horizon3.ai/attack-research/disclosures/unsafe-at-any-speed-abusing-python-exec-for-unauth-rce-in-langflow-ai/

https://search.censys.io/search?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=EXCLUDE&q=services.http.response.body%3Alangflow

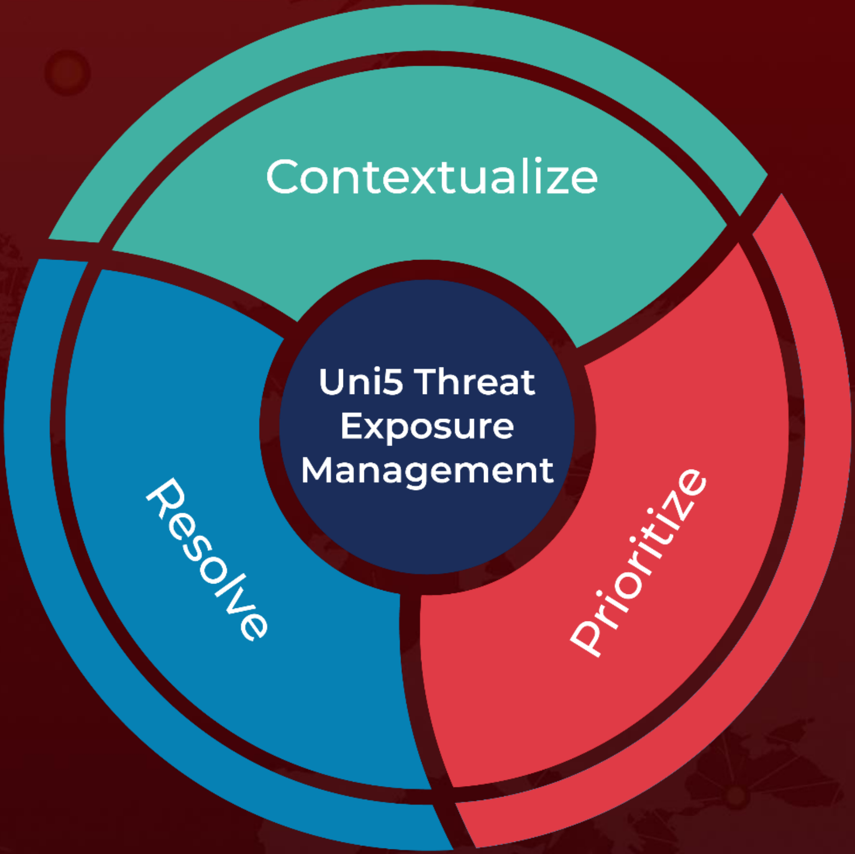
https://isc.sans.edu/diary/Exploit%2BAttempts%2Bfor%2BRecent%2BLangflow%2BAI%2BVulnerability%2BCVE20253248/31850/

https://github.com/langflow-ai/langflow/pull/6911/files

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 6, 2025 • 7:30 AM

More at www.hivepro.com