Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-3248 in Langflow Actively Exploited by Flodrix Botnet

Date of Publication	Date of Publication	Admiralty Code	TA Number
May 6, 2025	June 19, 2025	A1	TA2025137

Summary

First Seen: February 22, 2025
Affected Product: Langflow
Malware: Flodrix botnet
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 attacks, including Flodrix botnet infections, are targeting publicly accessible Langflow instances. 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 is exposed and lacks sandboxing, the attack requires no user interaction and is trivially exploitable.

#3 The vulnerability has a CVSS score of 9.8, reflecting its critical severity and ease of exploitation. Successful exploitation allows full OS-level control, enabling attackers to read sensitive files (e.g., /etc/passwd), deploy malware, exfiltrate data, and move laterally within the network.

#4 Active exploitation of CVE-2025-3248 has been observed in the wild. Mass scanning from TOR exit nodes has been detected, alongside attacks aimed at reading environment variables and system files. Notably, the Flodrix botnet is actively exploiting this flaw to infect vulnerable Langflow servers. The botnet leverages downloader scripts, often deceptively named “docker”, to retrieve and execute ELF binaries across various architectures. Flodrix exhibits anti-forensic and stealth capabilities, including process obfuscation, self-deletion, and C2-based command retrieval.

#5 As of June 2025, over 900 Langflow instances remain publicly exposed, with hundreds of malicious IPs actively probing for this vulnerability. This incident highlights the urgent need for secure coding practices, particularly regarding input validation, authentication, and sandboxing in AI platforms that process 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	TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact
TA0043 Reconnaissance	TA0007 Discovery	T1204 User Execution	T1588.006 Vulnerabilities
T1210 Exploitation of Remote Services	T1588 Obtain Capabilities	T1588.005 Exploits	T1059.006 Python
T1595 Active Scanning	T1595.002 Vulnerability Scanning	T1498 Network Denial of Service	T1041 Exfiltration Over C2 Channel
T1070 Indicator Removal	T1071.001 Web Protocols	T1071 Application Layer Protocol	T1059 Command and Scripting Interpreter
T1033 System Owner/User Discovery	T1027 Obfuscated Files or Information	T1204.002 Malicious File	T1190 Exploit Public-Facing Application

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	EC0F2960164CDCF265ED78E66476459337C03ACB469B6B302E1E8AE01C35D7EC, 52A034E732BCE0CB10FBFAE6F3C208FFB885D490FBCD70BAD62FB2E32A7C33F8, E4AEA6EE7005EE4B500E0B8673B69EA91D1A7532FACAD653E575BA29824845D9, 7BDBF2766AD55F9A67BFBB97A32D308530E4B5959BB68A9ACB22326DFEE8F282, E08E03091DEFB5006792934389AA350E8C48C37E59E282EF8FE3C3F126212E20, 57CEDC81378F98E568539CC653349FF70EF851A6D51886FD2560F30DF5E31BBD, C97128A452FF24D9BA70A3A7674C1D7AD21BABC9C75E7C34330BADDAEEA3D4BD, 80C956C5F279A436E7CF81B3E47333144DA5EF39BD76BD8C4A65E4571125EA7A, DC9A484F4910EE08EB22AFAB8D328EEF5328C9A5A8ABC6A50062E2065262A81F, 4AA59DDE4C8DA2CFF1A3AFE02DB3AE6C00D99E698DB11838B791E1D6C582FFB6, 912573354E6ED5D744F490847B66CB63654D037EF595C147FC5A4369FEF3BFEE, 09EFD15FF0317424B9B964626DA5E42D68B3CE91F509B16DAD9892D156D3EABE, 1E5E9723C6B492C477471CCCB4D7B26AAE653B0C5491C29739F784C664699D36, AB0F9774CA88994091DB0AE328D98F45034F653BD34E4F5E85679A972D3A039C, C2BCDD6E3CC82C4C4DB6AAF8018B8484407A3E3FCE8F60828D2087B2568ECCA4, A6CF8124E9B4558AACC7DDFA24B440454B904B937929BE203ED088B1040D1B36, EC52F75268B2F04B84A85E08D56581316BD5CCFEB977E002EB43270FE713F307, CCB02DCE1BCA9C3869E1E1D1774764E82206026378D1250AED324F1B7F9B1F11, 9991C664C052EC407E53439AC6BB4DF3CBBE3E54AF243D007A39D8A3DAB935B9, F73B554E6AA7095CFC79CDB687204D99533AEDA73309106BA6CC9428FF57BD1E, EE84591092A971C965B4E88CC5D6E8C2F07773B3BEE1486F3A52483EE72A2B3B,

TYPE	VALUE
SHA256	C2DCEB14EB91802CD4F78E78634E7837F4B2F4D1329D3F5293C53798B4D0C30E, 9850EB26D8CBEF3358DA4DF154E054759A062116C2AA82DE9A69A8589F0DCE49, A42F8428AA75C180C2F89FBB8B1E44307C2390ED0EBF5AF10015131B5494F9E1, E1C830643DE2EC7BC7C032F7EC96C302CE54E703EAF576D3796D1BBD05D8A63F, 51085CD2DE0ED6A9A6738AC85A8CAF297FBD22DB4B049822A9802BB8140DCD3D, 64927195D388BF6A1042C4D689BCB2C218320E2FA93A2DCC065571ADE3BB3BD3, ABB0C4AD31F013DF5037593574BE3207A4C1E066A96E58CE243AAF2EF0FC0E4D, 47497B24AF6FF42DAE582998AEEEDBC7B9CA6B3E0D82E8E49E8AC4A0F453A659, DF9E9006A566A4FE30EAA48459EC236D90FD628F7587DA9E4A6A76D14F0E9C98, 002F3B2C632E0BE6CBC3FDF8AFCD0432FFE36604BA1BA84923CADAA147418187, 99B59E53010D58F47D332B683EB8A40DF0E0EACEF86390BCA249A708E47D9BAD, 78B430BFF7D797B020D06702659E26D8CA01C8FC968239390697AEFF472623A7, D8D5A32BBD747C92FA1BB55DCE4ABB20E8D09711AEBCBFE8E7EEC83173F9E627, 08CF20E54C634F21D8708573EEF7FDE4DBD5D3CD270D2CB8790E3FE1F42ECCEC, 6DD0464DD0ECDE4BB5A769C802D11AB4B36BBE0DD4F0F44144121762737A6BE0, C462A09DB1A74DC3D8ED199EDCA97DE87B6ED25C2273C4A3AFE811ED0C1C8B1D,
MD5	Eaf854b9d232566e82a805e9be8b2bf2, 176f293dd15b9cf87ff1b8ba70d98bcf, 82d8bc51a89118e599189b759572459f
SHA1	E367cee9e02690509b4acdf7060f1a4387d85ec7, 7823b91efceedaf0e81856c735f13ae45b494909, d703ec4c4d11c7a7fc2fcf4a4b8776862a3000b5
IPv4	80[.]66[.]75[.]121, 188[.]166[.]68[.]21, 206[.]71[.]149[.]179,

TYPE	VALUE
IPv4	45[.]61[.]137[.]226, 139[.]59[.]223[.]9, 35[.]221[.]194[.]209, 204[.]216[.]147[.]144, 45[.]33[.]95[.]165, 3[.]35[.]37[.]70

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

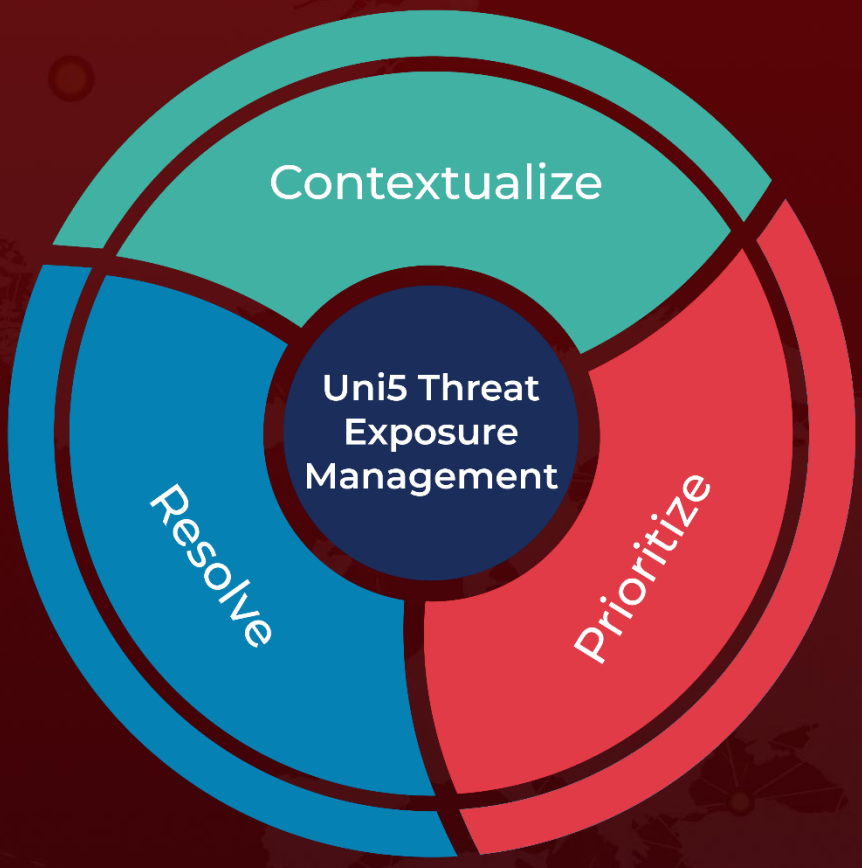
https://www.recordedfuture.com/blog/langflow-cve-2025-3248

https://www.trendmicro.com/en_us/research/25/f/langflow-vulnerability-flodric-botnet.html

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