

HiveForce Labs

THREAT ADVISORY



VULNERABILITY REPORT

LangGrinch: Critical LangChain Serialization Flaws Enable Secret Exfiltration

Date of Publication

December 30, 2025

Admiralty Code

A1

TA Number

TA2025393







Summary

First Seen: December 4, 2025

Affected Products: LangChain

Impact: CVE-2025-68664, codenamed "LangGrinch," is a critical serialization injection vulnerability (CVSS 9.3) in LangChain Core, one of the most widely deployed AI frameworks with over 847 million downloads. The flaw allows attackers to inject malicious data through AI model outputs or user inputs, which the application then mistakenly processes as trusted commands, enabling secret extraction from environment variables, unauthorized object instantiation, and potential remote code execution. A parallel vulnerability (CVE-2025-68665) affects LangChain.js with similar mechanics. Proof-of-concept exploits are available and the attack is automatable. Organizations should upgrade to langchain-core versions 0.3.81 or 1.2.5 immediately.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-68664	LangGrinch (LangChain Serialization Injection Vulnerability)	LangChain			
CVE-2025-68665	LangChain Serialization Injection Vulnerability	LangChain			

Vulnerability Details

#1

CVE-2025-68664, codenamed "LangGrinch," is a critical vulnerability in LangChain Core with a CVSS score of 9.3. LangChain is one of the most widely used frameworks for building AI-powered applications, with approximately 847 million total downloads. The vulnerability was discovered by security researcher on December 4, 2025 and publicly disclosed on December 23, 2025. LangChain awarded a record \$4,000 bounty for this finding.

#2

The flaw exists in how LangChain handles data serialization—the process of converting data into a storable format and back. Attackers can exploit this by injecting specially crafted data through AI model responses or user inputs. When the application processes this malicious data, it mistakenly treats it as trusted internal commands rather than user input. This can allow attackers to steal sensitive secrets like API keys and passwords stored in environment variables, create unauthorized objects within the application, and potentially execute malicious code on the server.

#3

Organizations at risk include those using LangChain for AI applications that process streaming outputs, store conversation history, use caching, or run logging pipelines. A similar vulnerability (CVE-2025-68665) also affects LangChain.js, meaning teams running both Python and JavaScript implementations should treat this as a coordinated risk. Proof-of-concept exploits are available and the attack can be automated, increasing the urgency for remediation.

#4

Affected versions include langchain-core prior to 0.3.81 and 1.2.5. Organizations should upgrade immediately, review any systems that process AI-generated content, and ensure environment variables containing secrets are properly protected.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-68664	Langchain-core versions before: 0.3.81 and 1.2.5	cpe:2.3:a:langchain-ai:langchain:*:*:*:*:*.*	CWE-502
CVE-2025-68665	Langchain-core versions before: 0.3.80 and 1.1.8, and Langchain versions before: 0.3.37 and 1.2.3	cpe:2.3:a:langchain-ai:langchainjs:*:*:*:*:*.*.*.*	CWE-502

Recommendations



Immediate Patch Deployment: Immediately upgrade all affected LangChain components to their patched versions. For Python environments, update langchain-core to version 1.2.5 or later (or 0.3.81+ for legacy branches). For JavaScript/TypeScript deployments, upgrade @langchain/core and langchain to their respective fixed releases. Treat this as a critical security update due to the availability of public proof-of-concept exploits.



Implement Mitigation Controls: Use the new `allowed_objects` parameter to restrict deserializable classes. Treat all LLM outputs as untrusted input, including metadata fields. Sandbox deserialization operations in restricted environments. Log and alert on deserialization operations involving unexpected object types. Audit stored/cached LangChain objects for potential malicious payloads.



Enhanced Monitoring and Detection: Monitor for unusual `lc` key structures in serialized data. Review logs for deserialization of unexpected object types. Configure SIEM rules to detect exploitation attempts and indicators of compromise. Enable detailed audit logging for serialization and deserialization events.



Proactive Security Measures: Establish AI security guidelines documenting and enforcing security boundaries for AI application data flows. Add automated vulnerability scanning for AI/ML framework dependencies. Perform regular security assessments of serialization/deserialization patterns. Educate developers on serialization injection risks in AI frameworks. Implement multiple security layers including input validation, output encoding, and runtime monitoring. Track security advisories for LangChain and related AI frameworks.



Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	<u>T1190</u> : Exploit Public-Facing Application	
Execution	<u>T1059</u> : Command and Scripting Interpreter	<u>T1059.006</u> : Python
Credential Access	<u>T1552</u> : Unsecured Credentials	<u>T1552.001</u> : Credentials In Files
	<u>T1078</u> : Valid Accounts	
Defense Evasion	<u>T1027</u> : Obfuscated Files or Information	
Discovery	<u>T1082</u> : System Information Discovery	
Resource Development	<u>T1588</u> : Obtain Capabilities	<u>T1588.007</u> : Artificial Intelligence



Patch Link

<https://github.com/langchain-ai/langchain/releases>



References

<https://github.com/langchain-ai/langchainjs/security/advisories/GHSA-r399-636x-v7f6>

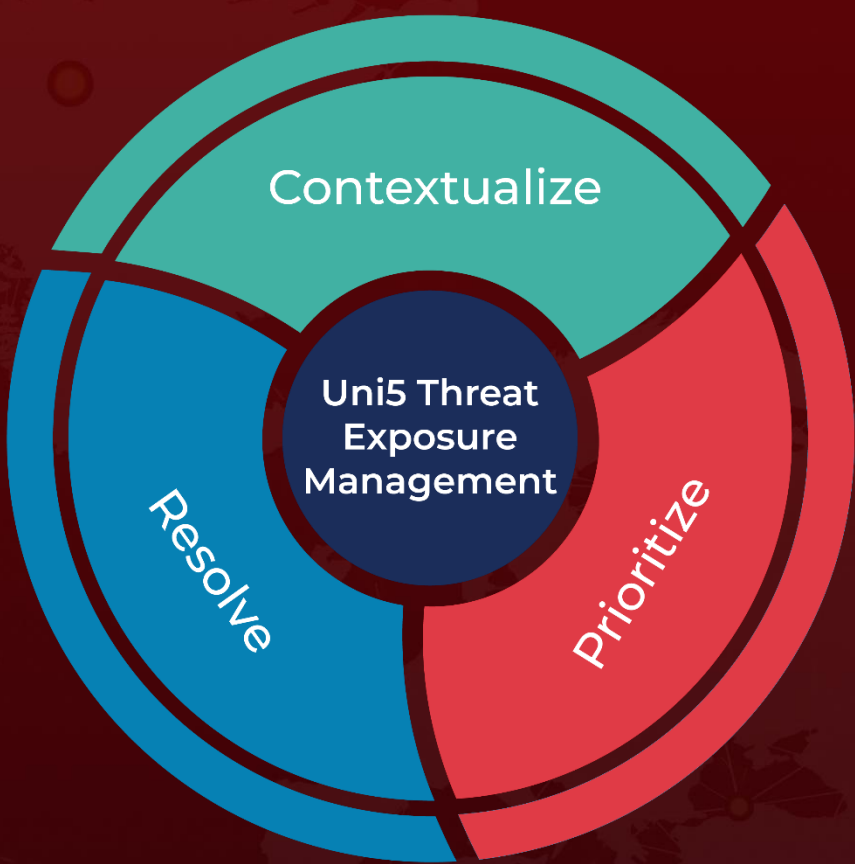
<https://cyata.ai/blog/langgrinch-langchain-core-cve-2025-68664/>



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
December 30, 2025 • 5:30 AM

