# CVE Detail – CVE-2024-4181

A command injection vulnerability exists in the RunGptLLM class of the llama\_index library, version 0.9.47, used by the RunGpt framework from JinaAI to connect to Language Learning Models (LLMs). The vulnerability arises from the improper use of the eval function, allowing a malicious or compromised LLM hosting provider to execute arbitrary commands on the client's machine. This issue was fixed in version 0.10.13. The exploitation of this vulnerability could lead to a hosting provider gaining full control over client machines.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.6393

## CVSS Scoring

CVSS v3.0 Score: 8.8

Severity: HIGH

## Mapped CWE(s)

* CWE-94: Improper Control of Generation of Code ('Code Injection')

## CAPEC(s)

* CAPEC-242: Code Injection
* CAPEC-35: Leverage Executable Code in Non-Executable Files
* CAPEC-77: Manipulating User-Controlled Variables

## ATT&CK Techniques

* T1027.009: Embedded Payloads
* T1564.009: Resource Forking
* T1027.006: HTML Smuggling

## Used By (Actors/Tools)

* Pikabot (malware)
* macOS.OSAMiner (malware)
* EnvyScout (malware)
* Emotet (malware)
* DUSTTRAP (malware)
* BADHATCH (malware)
* DUSTPAN (malware)
* Moneybird (malware)
* Keydnap (malware)
* IcedID (malware)
* CHIMNEYSWEEP (malware)
* MultiLayer Wiper (malware)
* Netwalker (malware)
* SMOKEDHAM (malware)
* Uroburos (malware)
* DEADEYE (malware)
* ComRAT (malware)
* QakBot (malware)
* OSX/Shlayer (malware)
* DEADWOOD (malware)
* Dtrack (malware)
* Invoke-PSImage (tool)
* Lazarus Group (intrusion-set)
* TA577 (intrusion-set)
* APT29 (intrusion-set)
* C0021 (campaign)
* Moonstone Sleet (intrusion-set)