



CVE-2023-29374

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-29374
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-05 02:15:00 UTC
Updated	2023-04-17 16:57:00 UTC
Description	In LangChain through 0.0.131, the LLMMathChain chain allows prompt injection attacks that can execute arbitrary code via

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Langchain	Langchain	All	All	All	All

References

Reference
Patch LLMMathChain exec vulnerability by zachschillaci27 · Pull Request #1119 · hwchase17/langchain · GitHub
Exploiting llm-math (and likely PAL) and suggesting an alternative · Issue #814 · hwchase17/langchain · GitHub
Security concerns · Issue #1026 · hwchase17/langchain · GitHub
Rich Harang (@rharang@mastodon.social) on Twitter: "this is why we can't have nice things. A langchain LLM agent for solving math problem"
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report