CVE-2023-36095

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-36095
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-05 03:15:00 UTC
Updated	2023-08-14 18:15:00 UTC
Description	An issue in Harrison Chase langchain v.0.0.194 allows an attacker to execute arbitrary code via the python exec calls in the

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Langchain	Langchain	0.0.194	All	All	All

References

Reference	So
LangChain	MI
Prompt injection which leads to arbitrary code execution in `langchain.chains.PALChain` · Issue #5872 · langchain-ai/langchain · GitHub	MI
GitHub - langchain-ai/langchain: ⚡ Building applications with LLMs through composability ⚡	MI
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

994795 Python (Pip) Security Update for langchain (GHSA-gwqq-6vq7-5j86)

Free CVE JSON API cve.report/api

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