



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	Source
LangChain	MISC
Prompt injection which leads to arbitrary code execution in `langchain.chains.PALChain` · Issue #5872 · langchain-ai/langchain · GitHub	MISC
GitHub - langchain-ai/langchain: < Building applications with LLMs through composability >	MISC
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)

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