CVE-2023-38896

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

Summary

CVE	CVE-2023-38896
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-15 17:15:00 UTC
Updated	2023-08-22 13:30:00 UTC
Description	An issue in Harrison Chase langchain v.0.0.194 and before allows a remote attacker to execute arbitrary code via the from_

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	Sou
JavaScript is not available.	MIS
Mitigate issue #5872 (Prompt injection -> RCE in PAL chain) by boazwasserman · Pull Request #6003 · hwchase17/langchain · GitHub	MIS
Prompt injection which leads to arbitrary code execution in `langchain.chains.PALChain` · Issue #5872 · hwchase17/langchain · GitHub	MIS
CVE Program record	CVI
NVD vulnerability detail	NVI

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

994866 Python (Pip) Security Update for langchain (GHSA-92j5-3459-qgp4)

Free CVE JSON API cve.report/api

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