



# CVE-2023-38896

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-38896
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-08-15 17:15:00 UTC
<b>Updated</b>	2023-08-22 13:30:00 UTC
<b>Description</b>	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	Source
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)

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](#)