



# LangChain Community: redirect chaining can lead to SSRF bypass via RecursiveUrlLoader

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

## Summary

<b>CVE</b>	CVE-2026-27795
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-02-25 18:23:41 UTC
<b>Updated</b>	2026-04-13 14:15:35 UTC
<b>Description</b>	LangChain is a framework for building LLM-powered applications. Prior to version 1.1.8, a redirect-based Server-Side Request Forgery (SSRF) bypass was possible via RecursiveUrlLoader.

## Risk And Classification

**Primary CVSS:** v3.1 7.4 HIGH from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

**EPSS:** 0.000420000 probability, percentile 0.125120000 (date 2026-04-15)

**Problem Types:** CWE-918 | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.4	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N
3.1	security-advisories@github.com	Secondary	4.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:N/A:N
3.1	CNA	DECLARED	4.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

### NVD Known Affected Configurations (CPE 2.3)

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Langchain-ai	Langchainjs	affected < 1.1.18	Not specified

### References

Reference	Source	Link	Tags
github.com/langchain-ai/langchainjs/pull/9990	security-advisories@github.com	github.com	Issue T
github.com/langchain-ai/langchainjs/security/advisories/GHSA-gf3v-fwqg-4vh7	security-advisories@github.com	github.com	Not Ap
github.com/langchain-ai/langchainjs/commit/d5e3db0d01ab321ec70a875805b2f...	security-advisories@github.com	github.com	Patch
github.com/langchain-ai/langchainjs/commit/2812d2b2b9fd9343c4850e2ab906b...	security-advisories@github.com	github.com	Patch
github.com/langchain-ai/langchainjs/releases/tag/%40langchain%2Fcommunit...	security-advisories@github.com	github.com	Releas
github.com/langchain-ai/langchainjs/releases/tag/%40langchain%2Fcommunit...	security-advisories@github.com	github.com	Releas
github.com/langchain-ai/langchainjs/security/advisories/GHSA-mpfv-75cg-56wg	security-advisories@github.com	github.com	Vendor
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)