



# locize Client SDK: Cross-origin DOM XSS & Handler Hijack Through Missing e.origin Validation in InContext Editor

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

## Summary

<b>CVE</b>	CVE-2026-41886
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-08 16:16:12 UTC
<b>Updated</b>	2026-05-08 16:16:12 UTC
<b>Description</b>	locize is a localization platform that connects code and i18n setup. Prior to version 4.0.21, the locize client SDK registers a

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from security-advisories@github.com

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

**EPSS:** 0.000150000 probability, percentile 0.032660000 (date 2026-05-12)

**Problem Types:** CWE-79 | CWE-346 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | CWE-346 CWE-346: Origin Validation Error

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:H/A:L
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:H/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Score

Changed

Confidentiality

Low

Integrity

High

Availability

Low

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Locize	Locize	affected < 4.0.21	Not specified

### References

Reference	Source	Link	Tags
github.com/locize/locize/security/advisories/GHSA-w937-fg2h-xhq2	security-advisories@github.com	github.com	
github.com/locize/locize/releases/tag/v4.0.21	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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)