



# Locutus Prototype Pollution due to incomplete fix for CVE-2026-25521

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

## Summary

<b>CVE</b>	CVE-2026-33994
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-27 23:17:14 UTC
<b>Updated</b>	2026-04-01 14:16:51 UTC
<b>Description</b>	Locutus brings stdlibs of other programming languages to JavaScript for educational purposes. Starting in version 2.0.39 ar

## Risk And Classification

**Primary CVSS:** v4.0 6.3 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000460000 probability, percentile 0.140430000 (date 2026-04-01)

**Problem Types:** CWE-1321 | CWE-1321 CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Locutus	Locutus	All	All	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Locutusjs</a>	<a href="#">Locutus</a>	affected >= 2.0.39, < 3.0.25	Not specified

## References

Reference	Source	Link	Tags
<a href="https://github.com/locutusjs/locutus/security/advisories/GHSA-vc8f-x9pp-wf5p">github.com/locutusjs/locutus/security/advisories/GHSA-vc8f-x9pp-wf5p</a>	<a href="mailto:security-advisories@github.com">security-advisories@github.com</a>	<a href="https://github.com">github.com</a>	Exploit, V
<a href="https://github.com/locutusjs/locutus/commit/345a6211e1e6f939f96a7090bfeff642c9fc...">github.com/locutusjs/locutus/commit/345a6211e1e6f939f96a7090bfeff642c9fc...</a>	<a href="mailto:security-advisories@github.com">security-advisories@github.com</a>	<a href="https://github.com">github.com</a>	Patch
<a href="https://github.com/locutusjs/locutus/pull/597">github.com/locutusjs/locutus/pull/597</a>	<a href="mailto:security-advisories@github.com">security-advisories@github.com</a>	<a href="https://github.com">github.com</a>	Issue Tra
<a href="https://github.com/locutusjs/locutus/releases/tag/v3.0.25">github.com/locutusjs/locutus/releases/tag/v3.0.25</a>	<a href="mailto:security-advisories@github.com">security-advisories@github.com</a>	<a href="https://github.com">github.com</a>	Release
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonica

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](#).

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