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

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-33994
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 23:17:14 UTC
Updated	2026-04-01 14:16:51 UTC
Description	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/MSC:X/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/V
4.0	CNA	DECLARED	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/V
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/MSC:X/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	Locutusjs	Locutus	affected >= 2.0.39, < 3.0.25	Not specified

References

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

No vendor comments have been submitted for this CVE.

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