



Express XSS Sanitizer: allowedTags/allowedAttributes bypass leads to permissive sanitization (XSS risk)

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

Summary

CVE CVE-2026-33979**State** PUBLISHED**Assigner** GitHub_M**Source Priority** CVE Program / NVD first with legacy fallback**Published** 2026-03-27 22:16:22 UTC**Updated** 2026-03-31 18:24:58 UTC**Description** Express XSS Sanitizer is Express 4.x and 5.x middleware which sanitizes user input data (in req.body, req.query, req.head

Risk And Classification

Primary CVSS: v3.1 8.2 HIGH from security-advisories@github.com**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N**EPSS:** 0.000100000 probability, percentile 0.010110000 (date 2026-04-01)

Problem Types: CWE-79 | CWE-183 | CWE-183 CWE-183: Permissive List of Allowed Inputs | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N
3.1	CNA	DECLARED	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Express Xss Sanitizer Project	Express Xss Sanitizer	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	AhmedAdelFahim	Express-xss-sanitizer	affected < 2.0.2	Not specified

References

Reference	Source	Link	Tags
github.com/AhmedAdelFahim/express-xss-sanitizer/commit/5623009ef11dcf095...	security-advisories@github.com	github.com	Patch
github.com/AhmedAdelFahim/express-xss-sanitizer/releases/tag/v2.0.2	security-advisories@github.com	github.com	Product
github.com/AhmedAdelFahim/express-xss-sanitizer/security/advisories/GHSA...	security-advisories@github.com	github.com	Exploit
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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