Rails has a possible XSS vulnerability in its Action View tag helpers

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-33168
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-23 23:17:12 UTC
Updated	2026-04-16 14:46:24 UTC
Description	Action View provides conventions and helpers for building web pages with the Rails framework. Prior to versions 8.1.2.1, 8.

Risk And Classification

Primary CVSS: v4.0 2.3 LOW from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/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: 0.000230000 probability, percentile 0.063620000 (date 2026-04-21)

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

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	2.3	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI
4.0	CNA	DECLARED	2.3	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Passive

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Rails	Actionview	affected >= 8.1.0.beta1, < 8.1.2.1	Not specified
CNA	Rails	Actionview	affected >= 8.0.0.beta1, < 8.0.4.1	Not specified
CNA	Rails	Actionview	affected < 7.2.3.1	Not specified

References

Reference	Source	Link	Tags
github.com/rails/rails/commit/c79a07df1e88738df8f68cb0ee759ad6128ca924	security-advisories@github.com	github.com	
github.com/rails/rails/commit/63f5ad83edaa0b976f82d46988d745426aa4a42d	security-advisories@github.com	github.com	
github.com/rails/rails/security/advisories/GHSA-v55j-83pf-r9cq	security-advisories@github.com	github.com	
github.com/rails/rails/commit/0b6f8002b52b9c606fd6be9e7915d9f944cf539c	security-advisories@github.com	github.com	
github.com/rails/rails/releases/tag/v7.2.3.1	security-advisories@github.com	github.com	
github.com/rails/rails/releases/tag/v8.0.4.1	security-advisories@github.com	github.com	
github.com/rails/rails/releases/tag/v8.1.2.1	security-advisories@github.com	github.com	
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report