



Matomo <= 4.15.3 - Reflected Cross-Site Scripting via idsite

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2023-6923
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-02-29 01:42:49 UTC
Updated	2026-04-08 17:17:17 UTC

Description The Matomo Analytics – Ethical Stats. Powerful Insights. plugin for WordPress is vulnerable to Reflected Cross-Site Scripting (XSS) via the idsite parameter. An attacker can inject arbitrary HTML and JavaScript code into the page, which is then rendered by the browser. This can lead to session hijacking, defacement, and other malicious activities.

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

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

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
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	security@wordfence.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Matomoteam	Matomo Analytics Powerful Privacy-First Insights For WordPress	affected 4.15.3 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	plugins.tr
www.wordfence.com/threat-intel/vulnerabilities/id/2e2d54eb-c176-49c4-a4fc-833e1...	af854a3a-2127-422b-91ae-364da2661108	www.wor
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: Felipe Restrepo Rodriguez (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-02-07T00:00:00.000Z	Disclosed

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

[site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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