



Yay! Forms | Embed Custom Forms, Surveys, and Quizzes Easily <= 1.2.1 - Authenticated (Contributor+) Stored Cross-Site Scripting

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2024-12522
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-02-19 08:15:14 UTC
Updated	2026-04-08 18:19:50 UTC
Description	The Yay! Forms Embed Custom Forms, Surveys, and Quizzes Easily plugin for WordPress is vulnerable to Stored Cross-Site Scripting (XSS) via the 'Authenticated (Contributor+)' user role. An attacker can inject malicious JavaScript code into the plugin's output, which is then executed in the browser of any user viewing the affected page.

Risk And Classification

Primary CVSS: v3.1 6.4 MEDIUM from security@wordfence.com

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

EPSS: 0.001110000 probability, percentile 0.295400000 (date 2026-04-08)

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	security@wordfence.com	Secondary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

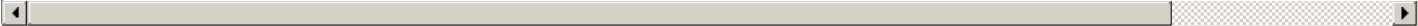


Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Yayforms	Yay! Forms	affected 1.2.1 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/yayforms/tags/1.2.1/yayforms.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.trac.wordpress.org
www.wordfence.com/threat-intel/vulnerabilities/id/461ab75a-3ced-4296-9dc1-b8eee...	security@wordfence.com	www.wordfence.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov



Vendor Comments And Credit

Discovery Credit
CNA: Peter Thaleikis (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-02-18T19:30:41.000Z	Disclosed

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

