



Cognito Forms <= 2.0.7 - Authenticated (Contributor+) Stored Cross-Site Scripting via id Parameter

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

Summary

CVE	CVE-2024-10182
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-12 05:15:05 UTC
Updated	2026-04-08 18:19:04 UTC
Description	The Cognito Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to 2.0.7. An authenticated user with Contributor+ or higher permissions can inject arbitrary HTML and JavaScript into the page content, which is then rendered to all users. This can be used to steal session cookies, perform actions on behalf of the user, or deface the site.

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: 0.005540000 probability, percentile 0.680740000 (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	Cognitoapps	Cognito Forms	affected 2.0.7 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/cognito-forms/trunk/cognito-forms.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/cognito-forms/trunk/api.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/cognito-forms/trunk/cognito-forms.php	security@wordfence.com	plugins.trac.wordpress.org
www.wordfence.com/threat-intel/vulnerabilities/id/80b1d728-b5aa-4811-b92a-9ce36...	security@wordfence.com	www.wordfence.com
wordpress.org/plugins/cognito-forms	security@wordfence.com	wordpress.org
plugins.trac.wordpress.org/browser/cognito-forms/trunk/api.php	security@wordfence.com	plugins.trac.wordpress.org
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	2024-12-11T15:39:58.000Z	Disclosed

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

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](#).

Free CVE JSON API cve.report/api

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