



Gravity Forms <= 2.9.30 - Unauthenticated Stored Cross-Site Scripting via Credit Card 'Card Type' Sub-Field

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

Summary

CVE	CVE-2026-4394
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 00:16:05 UTC
Updated	2026-04-08 21:26:35 UTC
Description	The Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Credit Card field's 'Card Type' sub-field.

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from security@wordfence.com

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

EPSS: 0.000840000 probability, percentile 0.244420000 (date 2026-04-14)

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	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	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

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Gravity Forms	Gravity Forms	affected 2.9.30 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/gravityforms/trunk/includes/fields/class-gf-field-cre...	security@wordfence.com	plugins.trac.wordpress.
plugins.trac.wordpress.org/browser/gravityforms/tags/2.9.25/includes/fields/class-gf-fie...	security@wordfence.com	plugins.trac.wordpress.
plugins.trac.wordpress.org/browser/gravityforms/tags/2.9.25/includes/fields/class-gf-fie...	security@wordfence.com	plugins.trac.wordpress.
plugins.trac.wordpress.org/browser/gravityforms/trunk/includes/fields/class-gf-field-cre...	security@wordfence.com	plugins.trac.wordpress.
www.wordfence.com/threat-intel/vulnerabilities/id/6f38d7b7-6df6-47a2-a9ba-87ef1...	security@wordfence.com	www.wordfence.com
docs.gravityforms.com/gravityforms-change-log	security@wordfence.com	docs.gravityforms.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: tadokun (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-18T15:53:51.000Z	Vendor Notified
CNA	2026-04-07T10:47:07.000Z	Disclosed

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

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](#).

Free CVE JSON API cve.report/api

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