



# WordPress Contact Forms by Cimatti plugin <= 1.8.0 - Cross Site Scripting (XSS) vulnerability

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

## Summary

<b>CVE</b>	CVE-2024-30549
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-03-31 20:15:08 UTC
<b>Updated</b>	2026-04-28 13:16:44 UTC
<b>Description</b>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cimatti Contact Forms

## Risk And Classification

**Primary CVSS:** v3.1 4.8 MEDIUM from nvd@nist.gov

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

**Problem Types:** 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	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
3.1	audit@patchstack.com	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

Required

Scope

Changed

Confidentiality

Low  
 Integrity  
 Low  
 Availability  
 None

**CVSS:3.1/AV:N/AC:L/PR:H/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	Cimatti	Wordpress Contact Forms	All	All	All	All

---

**Vendor Declared Affected Products**

Source	Vendor	Product	Version	Platforms
CNA	Cimatti	Contact Forms By Cimatti	affected 1.8.0 custom	Not specified

---

**References**

Reference	Source	Link
patchstack.com/database/vulnerability/contact-forms/wordpress-contact-forms-...	af854a3a-2127-422b-91ae-364da2661108	patchstack.c
patchstack.com/database/Wordpress/Plugin/contact-forms/vulnerability/wordpre...	audit@patchstack.com	patchstack.c
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

---

**Vendor Comments And Credit**

Discovery Credit  
**CNA: Joel Indra | Patchstack Bug Bounty Program (en)**

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