



WordPress Crazy Call To Action Box plugin <= 1.0.5 - Cross Site Scripting (XSS) vulnerability

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

Summary

CVE	CVE-2024-49236
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-18 10:15:07 UTC
Updated	2026-04-01 16:18:28 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hafiz Uddin Ahmed Cr

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:L/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')

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/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	Hafizuddinahmed	Crazy Call To Action Box	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Hafiz Uddin Ahmed	Crazy Call To Action Box	affected 1.0.5 custom	Not specified

References				
Reference	Source	Link	Tags	
patchstack.com/database/Wordpress/Plugin/crazy-call-to-action-box/vulnerabil...	audit@patchstack.com	patchstack.com		
CVE Program record	CVE.ORG	www.cve.org	canonical	
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal	

Vendor Comments And Credit
Discovery Credit
CNA: SOPROBRO Patchstack Bug Bounty Program (en)

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