



WordPress Rescue Shortcodes Plugin <= 2.5 is vulnerable to Cross Site Scripting (XSS)

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2023-41728
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-02 08:15:38 UTC
Updated	2026-04-28 19:21:18 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rescue Themes Rescue

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 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	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
3.1	audit@patchstack.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L

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	Rescuethemes	Rescue Shortcodes	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Rescue Themes	Rescue Shortcodes	affected n/a 2.5 custom	Not specified

References

Reference	Source
WordPress Rescue Shortcodes plugin <= 2.5 - Cross Site Scripting (XSS) vulnerability - Patchstack	af854a3a-2127-422b-91ae-364da26611
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: yuyudhn (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 2.6 or a higher version.

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

Free CVE JSON API cve.report/api

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