



WordPress WP Forms Puzzle Captcha Plugin <= 4.1 is vulnerable to Cross Site Request Forgery (CSRF) leading to XSS

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2023-48278
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-30 17:15:11 UTC
Updated	2024-11-21 08:31:23 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in Nitin Rathod WP Forms Puzzle Captcha allows Stored XSS.This issue

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	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	audit@patchstack.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nitinrathod	Wp Forms Puzzle Captcha	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Nitin Rathod	WP Forms Puzzle Captcha	affected n/a 4.1 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/wp-forms-puzzle-captcha/wordpress-wp-f...	af854a3a-2127-422b-91ae-364da2661108	patchstack.
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: qilin_99 (Patchstack Alliance) (en)

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