



WordPress Yandex Site search pinger plugin <= 1.5 - Cross Site Scripting (XSS) vulnerability

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

Summary

CVE	CVE-2025-48352
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-08-28 13:15:54 UTC
Updated	2026-04-23 15:31:09 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sitesearch-yandex Yan

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from audit@patchstack.com

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

EPSS: 0.000390000 probability, percentile 0.116840000 (date 2026-05-17)

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	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

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Sitesearch-yandex	Yandex Site Search Pinger	affected 1.5 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/yandex-pinger/vulnerability/wordpre...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

Vendor Comments And Credit

Discovery Credit

CNA: [Nabil Irawan | Patchstack Bug Bounty Program \(en\)](#)

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