



# Yoast SEO <= 22.5 - Reflected Cross-Site Scripting

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

## Summary

<b>CVE</b>	CVE-2024-4041
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-05-14 15:42:45 UTC
<b>Updated</b>	2026-04-08 18:21:40 UTC
<b>Description</b>	The Yoast SEO plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via URLs in all versions up to, and incl

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from security@wordfence.com

**CVSS:3.1/AV:N/AC:L/PR:N/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	security@wordfence.com	Secondary	6.1	MEDIUM	<b>CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N</b>
3.1	CNA	DECLARED	6.1	MEDIUM	<b>CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N</b>

## 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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Yoast	Yoast SEO Advanced SEO With Real-time Guidance And Built-in AI	affected 22.5 semver	Not specified

### References

Reference	Source
plugins.trac.wordpress.org/browser/wordpress-seo/trunk/inc/class-wpseo-admin-bar-menu.php	af854a3a-2127-422b-91ae-364da2661108
www.wordfence.com/threat-intel/vulnerabilities/id/4e04b161-3cd0-454d-869c-56f42...	af854a3a-2127-422b-91ae-364da2661108
plugins.trac.wordpress.org/browser/wordpress-seo/trunk/inc/class-wpseo-shortlinker.php	af854a3a-2127-422b-91ae-364da2661108
plugins.trac.wordpress.org/changeset/3078555/wordpress-seo/trunk	af854a3a-2127-422b-91ae-364da2661108
plugins.trac.wordpress.org/browser/wordpress-seo/trunk/src/helpers/short-link-helper.php	af854a3a-2127-422b-91ae-364da2661108
plugins.trac.wordpress.org/browser/wordpress-seo/trunk/src/helpers/short-link-helper.php	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

### Vendor Comments And Credit

Discovery Credit

**CNA:** Bassem Essam (en)

### Additional Advisory Data

Source	Time	Event
CNA	2024-05-06T00:00:00.000Z	Disclosed

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

