

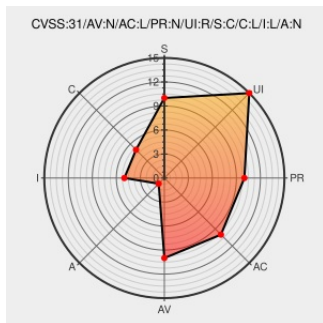


CVE-2021-24234

Published on: 04/22/2021 12:00:00 AM UTC

Last Modified on: 04/29/2021 06:47:00 PM UTC

CVE-2021-24234

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ivory Search](#) from [Ivorysearch](#) contain the following vulnerability:

The Search Forms page of the Ivory Search WordPress lugin before 4.6.1 did not properly sanitise the tab parameter before output it in the page, leading to a reflected Cross-Site Scripting issue when opening a malicious crafted link as a high privilege user. Knowledge of a form id is required to conduct the attack.

CVE-2021-24234 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Unknown - Ivory Search – WordPress Search Plugin** version < 4.6.1

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Reflected XSS Vulnerability found in Ivory Search	www.jinsonvarghese.com	MISC www.jinsonvarghese.com/reflected-xss-

Plugin

text/html

vulnerability-found-in-ivory-search-plugin/

Reflected XSS Vulnerability In Ivory Search WP Plugin Impact Over 60K sites

web.archive.org

text/html

Inactive Link

Not Archived

as119

MISC www.getastra.com/blog/911/plugin-exploit/reflected-xss-vulnerability-in-ivory-search-wp-plugin/

Attention Required! | Cloudflare

wpscan.com

text/html

Inactive Link

Not Archived

CONFIRM

wpscan.com/vulnerability/ecc620be-8e29-4860-9d32-86b5814a3835

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ivorysearch	Ivory Search	All	All	All	All

cpe:2.3:a:ivorysearch:ivory_search:*:*:*:*:*:wordpress:*:*

Discovery Credit

Jinson Varghese Behanan

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID →