

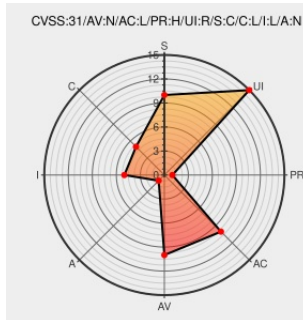


CVE-2021-25088

Published on: Not Yet Published

Last Modified on: 06/30/2022 02:24:00 PM UTC

CVE-2021-25088

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

Certain versions of [Google Xml Sitemaps](#) from [Google Xml Sitemaps Project](#) contain the following vulnerability:

The XML Sitemaps WordPress plugin before 4.1.3 does not sanitise and escape a settings before outputting it in the Debug page, which could allow high privilege users to perform Cross-Site Scripting attacks even when the `unfiltered_html` capability is disallowed (for example in multisite setup)

CVE-2021-25088 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Unknown - XML Sitemaps** version < 4.1.3

CVSS3 Score: **4.8 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link
Attention Required!	wpscan.com	MISC wpscan.com/vulnerability/820c51d6-186e-4d63-b4a7-

Cloudflare

text/htmlbd0a59c02cc8Inactive LinkNot Archived

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	Google Xml Sitemaps Project	Google Xml Sitemaps	All	All	All	All

cpe:2.3:a:google_xml_sitemaps_project:google_xml_sitemaps:*:*:*:*:wordpress:*:*:

Discovery Credit

JrXnm

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-25088 : The XML Sitemaps WordPress plugin before 4.1.3 does not sanitise and escape a settings before outp... twitter.com/i/web/status/1...	2022-06-20 10:36:56
/r/netcve	CVE-2021-25088	2022-06-20 11:38:57

← Previous ID

Next ID →