

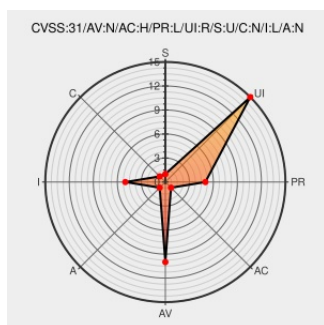


CVE-2021-4244

Published on: Not Yet Published

Last Modified on: 12/15/2022 07:53:00 PM UTC

CVE-2021-4244

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

Certain versions of [Easy Forms For Mailchimp](#) from [Yikesplugins](#) contain the following vulnerability:

A vulnerability classified as problematic has been found in yikes-inc-easy-mailchimp-extender Plugin up to 6.8.5. This affects an unknown part of the file admin/partials/ajax/add_field_to_form.php. The manipulation of the argument field_name/merge_tag/field_type/list_id leads to cross site scripting. It is possible to initiate the attack remotely.

Upgrading to version 6.8.6 is able to address this issue. The name of the patch is 3662c6593aa1bb4286781214891d26de2e947695. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-215307.

CVE-2021-4244 has been assigned by [cna@vuldb.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

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

CVE References

Description	Tags	Link
Fix Reflected Cross-Site Scripting issue by jpowersdev · Pull Request #889 · EvanHerman/yikes-inc-easy-mailchimp-extender · GitHub	github.com text/html	MISC github.com/EvanHerman/yikes-inc-easy-mailchimp-extender/pull/889
Release 6.8.6 · EvanHerman/yikes-inc-easy-mailchimp-extender · GitHub	github.com text/html	MISC github.com/EvanHerman/yikes-inc-easy-mailchimp-extender/releases/tag/6.8.6
CVE-2021-4244 yikes-inc-easy-mailchimp-extender Plugin add_field_to_form.php cross site scripting (ID 889)	vuldb.com text/html	MISC vuldb.com/?id.215307

Merge pull request #889 from yikesinc/fix/audit · EvanHerman/yikes-inc-easy-mailchimp-extender@3662c65 · GitHub

github.com
text/html

MISC github.com/EvanHerman/yikes-inc-easy-mailchimp-extender/commit/3662c6593aa1bb4286781214891d26de2e947695

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

Exploit/POC from Github

A vulnerability classified as problematic has been found in yikes-inc-easy-mailchimp-extender Plugin up to 6.8.5. Thi...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yikesplugins	Easy Forms For Mailchimp	All	All	All	All
cpe:2.3:a:yikesplugins:easy_forms_for_mailchimp:*:*:*:*:wordpress:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2021-4244	2022-12-12 14:40:23

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)