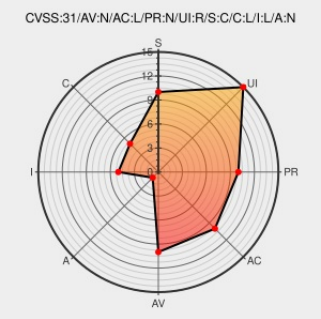
CVE-2021-24556

Published on: 08/23/2021 12:00:00 AM UTC

Last Modified on: 08/26/2021 11:18:00 PM UTC

CVE-2021-24556

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Email-subscriber from Email-subscriber Project contain the following vulnerability:

The kento_email_subscriber_ajax AJAX action of the Email Subscriber WordPress plugin through 1.1, does not properly sanitise, validate and escape the submitted subscribe_email and subscribe_name POST parameters, inserting them in the DB and then outputting them back in the Subscriber list (/wp-admin/edit.php?post_type=kes_campaign&page=kento_email_subscriber_list_settings), leading a Stored XSS issue.

CVE-2021-24556 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Unknown** - **Email Subscriber** version **<= 1.1**

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
wp-plugin : email-subscriber | Code Vigilant : to err is human.. To fix is Humanity	codevigilant.com text/html	MISC codevigilant.com/disclosure/2021/wp-plugin-email-subscriber/
Attention Required! | Cloudflare	wpscan.com text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/f050aedc-f79f-4b27-acac-0cdb33b25af8

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	Email-subscriber Project	Email-subscriber	All	All	All	All

cpe:2.3:a:email-subscriber_project:email-subscriber:*:*:*:*:*:wordpress:*:*:

Discovery Credit

Shreya Pohekar of Codevigilant Project

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-24556 : The kento_email_subscriber_ajax AJAX action of the Email Subscriber WordPress plugin through 1.1,… twitter.com/i/web/status/1…	2021-08-23 11:24:47
@LinInfoSec	Wordpress - CVE-2021-24556: codevigilant.com/disclosure/202…	2021-08-23 14:20:51

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report