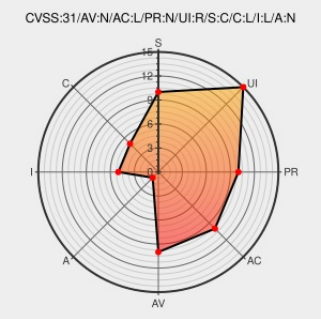
CVE-2021-39314

Published on: 12/14/2021 12:00:00 AM UTC

Last Modified on: 12/16/2021 02:54:00 PM UTC

CVE-2021-39314

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



Certain versions of Woo-enviopack from Wanderlust-webdesign contain the following vulnerability:

The WooCommerce EnvioPack WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the dataid parameter found in the ~/includes/functions.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.

CVE-2021-39314 has been assigned by security@wordfence.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **WooCommerce EnvioPack** - **WooCommerce EnvioPack** version **<= 1.2**

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
Vulnerability Advisories - Wordfence	www.wordfence.com text/html	MISC www.wordfence.com/vulnerability-advisories/#CVE-2021-39314

403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/browser/woo-enviopack/trunk/includes/functions.php?rev=2239846#L605

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wanderlust-webdesign	Woo-enviopack	All	All	All	All

cpe:2.3:a:wanderlust-webdesign:woo-enviopack:*:*:*:*:*:wordpress:*:*:

Discovery Credit

p7e4

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2021-39314	2021-12-14 16:39:21

← Previous ID

Next ID→