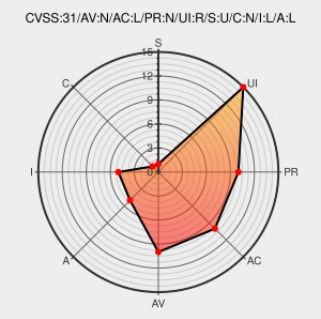
CVE-2022-46798

Published on: Not Yet Published

Last Modified on: 03/08/2023 08:06:00 PM UTC

CVE-2022-46798

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



Certain versions of Woolentor - Woocommerce Elementor Addons Builder from Hasthemes contain the following vulnerability:

Cross-Site Request Forgery (CSRF) vulnerability in HasThemes ShopLentor plugin <= 2.5.1 leading to plugin settings change.

CVE-2022-46798 has been assigned by audit@patchstack.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **HasThemes** - **ShopLentor** version **not down converted**

CVSS3 Score: 5.4 - MEDIUM

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

CVE References

Description	Tags	Link
WordPress WooLentor plugin <= 2.5.1 - CSRF Leading to Plugin Settings Change Vulnerability - Patchstack	patchstack.com text/html	MISC patchstack.com/database/vulnerability/woolentor-addons/wordpress-woolentor-plugin-2-5-1-csrf-leading-to-plugin-settings-change-vulnerability?_s_id=cve

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hasthemes	Woolentor - Woocommerce Elementor Addons Builder	All	All	All	All

cpe:2.3:a:hasthemes:woolentor_-_woocommerce_elementor_addons_\+_builder:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-46798 : Cross-Site Request Forgery CSRF vulnerability in HasThemes ShopLentor plugin <= 2.5.1 leading to… twitter.com/i/web/status/1…	2023-03-01 15:01:48
/r/netcve	CVE-2022-46798	2023-03-01 15:38:49

← Previous ID

Next ID→