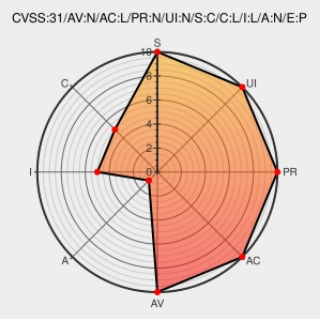
CVE-2020-28457

Published on: 12/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:26 PM UTC

CVE-2020-28457

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



Certain versions of S-cart from S-cart contain the following vulnerability:

This affects the package s-cart/core before 4.4. The search functionality of the admin dashboard in core/src/Admin/Controllers/AdminOrderController.phpindex is vulnerable to XSS.

CVE-2020-28457 has been assigned by report@snyk.io to track the vulnerability - currently rated as MEDIUM severity.

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
Cross-site Scripting (XSS) in s-cart/core | Snyk	Third Party Advisory, snyk.io, text/html	MISC snyk.io/vuln/SNYK-PHP-SCARTCORE-1047342
Hot fix error xss · s-cart/s-cart@4406d40 ·	Patch	MISC github.com/s-cart/s-

GitHub	Third Party Advisory github.com text/html	cart/commit/4406d407ad363ee7e4795ee290c9d2430b0413f8
XSS in admin dashboard · Issue #51 · s-cart/s-cart · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/s-cart/s-cart/issues/51
Release v4.4 · s-cart/s-cart · GitHub	Third Party Advisory github.com text/html	MISC github.com/s-cart/s-cart/releases/tag/v4.4

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	S-cart	S-cart	All	All	All	All
Application	S-cart	S-cart	All	All	All	All

cpe:2.3:a:s-cart:s-cart:*:*:*:*:*:*:*:*:

cpe:2.3:a:s-cart:s-cart:*:*:*:*:*:*:*:*:

Discovery Credit

Abdul Muhaimin

← Previous ID

Next ID→