



CVE-2017-10886

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-10886
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-17 14:29:00 UTC
Updated	2017-12-04 16:46:00 UTC
Description	Cross-site scripting vulnerability in CS-Cart Japanese Edition v4.3.10 and earlier (excluding v2 and v3), CS-Cart Multivendc

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cs-cart	Cs-cart	4.0.1	All	All	ja
Application	Cs-cart	Cs-cart	4.0.2	All	All	ja
Application	Cs-cart	Cs-cart	4.0.3	All	All	ja
Application	Cs-cart	Cs-cart	4.1.1	All	All	ja
Application	Cs-cart	Cs-cart	4.1.2	All	All	ja
Application	Cs-cart	Cs-cart	4.1.3	All	All	ja
Application	Cs-cart	Cs-cart	4.1.4	All	All	ja
Application	Cs-cart	Cs-cart	4.2.1	All	All	ja
Application	Cs-cart	Cs-cart	4.2.2	All	All	ja
Application	Cs-cart	Cs-cart	4.2.3	All	All	ja
Application	Cs-cart	Cs-cart	4.2.4	All	All	ja
Application	Cs-cart	Cs-cart	4.3.1	All	All	ja
Application	Cs-cart	Cs-cart	4.3.10	All	All	ja
Application	Cs-cart	Cs-cart	4.3.2	All	All	ja
Application	Cs-cart	Cs-cart	4.3.3	All	All	ja
Application	Cs-cart	Cs-cart	4.3.4	All	All	ja
Application	Cs-cart	Cs-cart	4.3.5	All	All	ja

Application	Cs-cart	Cs-cart	4.3.6	All	All	ja
Application	Cs-cart	Cs-cart	4.3.7	All	All	ja
Application	Cs-cart	Cs-cart	4.3.8	All	All	ja
Application	Cs-cart	Cs-cart	4.3.9	All	All	ja
Application	Cs-cart	Cs-cart	4.0.1	All	All	ja
Application	Cs-cart	Cs-cart	4.0.2	All	All	ja
Application	Cs-cart	Cs-cart	4.0.3	All	All	ja
Application	Cs-cart	Cs-cart	4.1.1	All	All	ja
Application	Cs-cart	Cs-cart	4.1.2	All	All	ja
Application	Cs-cart	Cs-cart	4.1.3	All	All	ja
Application	Cs-cart	Cs-cart	4.1.4	All	All	ja
Application	Cs-cart	Cs-cart	4.2.1	All	All	ja
Application	Cs-cart	Cs-cart	4.2.2	All	All	ja
Application	Cs-cart	Cs-cart	4.2.3	All	All	ja
Application	Cs-cart	Cs-cart	4.2.4	All	All	ja
Application	Cs-cart	Cs-cart	4.3.1	All	All	ja
Application	Cs-cart	Cs-cart	4.3.10	All	All	ja
Application	Cs-cart	Cs-cart	4.3.2	All	All	ja
Application	Cs-cart	Cs-cart	4.3.3	All	All	ja
Application	Cs-cart	Cs-cart	4.3.4	All	All	ja
Application	Cs-cart	Cs-cart	4.3.5	All	All	ja
Application	Cs-cart	Cs-cart	4.3.6	All	All	ja
Application	Cs-cart	Cs-cart	4.3.7	All	All	ja
Application	Cs-cart	Cs-cart	4.3.8	All	All	ja
Application	Cs-cart	Cs-cart	4.3.9	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.0.1	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.0.2	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.0.3	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.1.1	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.1.2	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.1.3	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.1.4	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.2.1	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.2.2	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.2.3	All	All	ja

Application	Cs-cart	Cs-cart Multivendor	4.2.4	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.1	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.10	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.2	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.3	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.4	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.5	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.6	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.7	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.8	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.9	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.0.1	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.0.2	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.0.3	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.1.1	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.1.2	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.1.3	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.1.4	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.2.1	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.2.2	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.2.3	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.2.4	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.1	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.10	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.2	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.3	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.4	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.5	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.6	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.7	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.8	All	All	ja
Application	Cs-cart	Cs-cart Multivendor	4.3.9	All	All	ja

References

Reference	Source	Link	Tags
セキュリティ :: 【JVN#29602086】 2017年11月13日に公表されたXSS脆弱性への対応方法 - ブログ記事	CONFIRM	tips.cs-cart.jp	Vulnerability

JVN#29602086: CS-Cart Japanese Edition vulnerable to cross-site scripting	JVN	jvn.jp	Third
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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