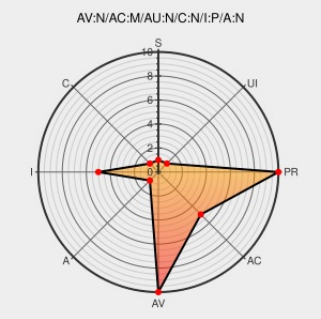
CVE-2014-8307

Published on: 10/16/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:50 PM UTC

CVE-2014-8307

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



Certain versions of Cart Engine from C97 contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in skins/default/outline.tpl in C97net Cart Engine before 4.0 allow remote attackers to inject arbitrary web script or HTML via the (1) path parameter in the "drop down TOP menu (with path)" section or (2) print_this_page variable in the footer_content_block section, as demonstrated by the QUERY_STRING to (a) index.php, (b) checkout.php, (c) contact.php, (d) detail.php, (e) distro.php, (f) newsletter.php, (g) page.php, (h) profile.php, (i) search.php, (j) sitemap.php, (k) task.php, or (l) tell.php.

CVE-2014-8307 has been assigned by cve@mitre.org to track the vulnerability

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
Full Disclosure: [Quantum Leap Advisory] #QLA140808 Cart Engine 3.0 Multiple vulnerabilities - SQL Injection, XSS Reflected, Open Redirect	Exploit, seclists.org, text/html	FULLDISC 20140916 [Quantum Leap Advisory] #QLA140808 Cart Engine 3.0 Multiple vulnerabilities - SQL Injection, XSS Reflected, Open Redirect
Cart Engine 3.0 Multiple vulnerabilities - Quantum Leap	Exploit, web.archive.org, text/html, Inactive Link, Not Archived	MISC www.quantumleap.it/cart-engine-3-0-multiple-vulnerabilities-sql-injection-reflected-xss-open-redirect

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	C97	Cart Engine	All	All	All	All

cpe:2.3:a:c97:cart_engine:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→