



CVE-2005-3997

Published on: 12/04/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

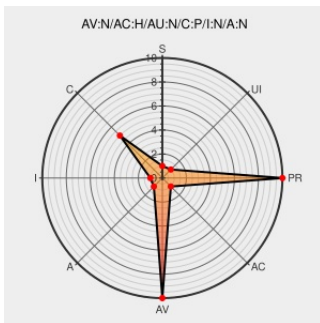
CVE-2005-3997

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Zen Cart](#) from [Zen Cart](#) contain the following vulnerability:

Zen Cart 1.2.6d and earlier, under certain PHP configurations, allows remote attackers to obtain sensitive information via direct requests to files in the admin/includes directory, including (1) graphs/banner_daily.php, (2) graphs/banner_infobox.php, (3) graphs/banner_yearly.php, (4) graphs/banner_monthly.php, (5)

application_bottom.php, (6) attributes_preview.php, (7) modules/category_product_listing.php, (8) modules/copy_to_confirm.php, (9) modules/delete_product_confirm.php, and (10) modules/move_product_confirm.php, which leaks the web server path in the resulting error message.

CVE-2005-3997 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.6 - LOW**

Access Vector

NETWORK

Access Complexity

HIGH

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

NONE

Availability Impact

NONE

CVE References

Description

Tags

Link

No Description Provided

[www.osvdb.org](#)

[OSVDB 22871](#)

Inactive Link Not Archived

No Description Provided

[www.osvdb.org](#)

[OSVDB 22869](#)

Inactive Link Not Archived

Secunia - Advisories - Zen Cart "admin_email"

[web.archive.org](#)

[SECUNIA 17869](#)

SQL Injection Vulnerability	text/html	
No Description Provided	www.osvdb.org	OSVDB 22873
	Inactive Link Not Archived	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2005-2728
No Description Provided	www.osvdb.org	OSVDB 22867
	Inactive Link Not Archived	
No Description Provided	www.osvdb.org	OSVDB 22874
	Inactive Link Not Archived	
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051205 = 1.2.6d blind SQL injection / remote commands execution:
No Description Provided	www.osvdb.org	OSVDB 22870
	Inactive Link Not Archived	
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051202 Zen-Cart <= 1.2.6d blind SQL injection / remote commands execution:
	rgod.altervista.org text/plain	MISC rgod.altervista.org/zencart_126d_xpl.html
	Inactive Link Not Archived	
No Description Provided	www.osvdb.org	OSVDB 22866
	Inactive Link Not Archived	
No Description Provided	www.osvdb.org	OSVDB 22875
	Inactive Link Not Archived	
No Description Provided	www.osvdb.org	OSVDB 22872
	Inactive Link Not Archived	
No Description Provided	www.osvdb.org	OSVDB 22868
	Inactive Link Not Archived	

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	Zen Cart	Zen Cart	All	All	All	All

cpe:2.3:a:zen_cart:zen_cart:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)