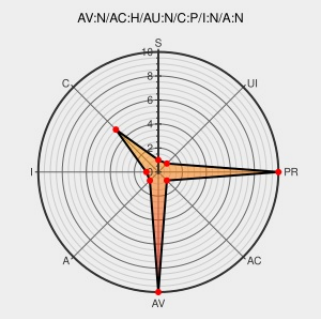
CVE-2005-3997

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 cve@mitre.org to track the vulnerability

CVSS2 Score: 2.6 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 22871
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 22869
Secunia - Advisories - Zen Cart "admin_email"	web.archive.org	SECUNIA 17869

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

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 and Source URL Uptime Status status.cve.report