



CVE-2005-1440

Published on: 05/03/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:25 PM UTC

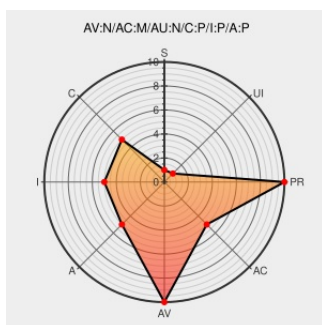
CVE-2005-1440

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Viart Shop Enterprise](#) from [Codetosell](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in ViArt Shop Enterprise 2.1.6 allow remote attackers to inject arbitrary web script or HTML via (1) various parameters to basket.php, (2) the nickname, email, topic, and message fields in forum.php, as demonstrated using forum_new_thread.php and forum_thread.php, (3) the page parameter

to page.php, (4) category_id and item_id parameters to reviews.php, (5) the category_id parameter to product_details.php, (6) the category_id or search_string parameters to products.php, or (7) the rp or page parameters to news_view.php.

CVE-2005-1440 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Lostmon's Blogger: ViArt Shop Enterprise multiple variable XSS

Exploit

[lostmon.blogspot.com](#)

[text/html](#)

MISC
[lostmon.blogspot.com/2005/04/viart-shop-enterprise-multiple.html](#)

No Description Provided

[www.osvdb.org](#)

OSVDB 15954

Inactive Link

Not Archived

No Description Provided

[www.osvdb.org](#)

OSVDB 15953

Inactive Link

Not Archived

Inactive Link Not Archived

No Description Provided

www.osvdb.org

OSVDB 15958

Inactive Link Not Archived

SecurityTracker.com Archives - ViArt Shop Input Validation Holes Permit Cross-Site Scripting Attacks

Exploit

securitytracker.com

text/html

SECTrack 1013853

No Description Provided

www.osvdb.org

OSVDB 15956

Inactive Link Not Archived

No Description Provided

Exploit

Vendor Advisory

www.osvdb.org

OSVDB 15951

Inactive Link Not Archived

Secunia - Advisories - ViArt Shop Enterprise Cross-Site Scripting and Script Insertion

web.archive.org

text/html

SECUNIA 15181

No Description Provided

www.osvdb.org

OSVDB 15952

Inactive Link Not Archived

No Description Provided

www.osvdb.org

OSVDB 15955

Inactive Link Not Archived

No Description Provided

www.osvdb.org

OSVDB 15957

Inactive Link Not Archived

CodeToSell ViArt Shop Enterprise Multiple Cross-Site Scripting and HTML Injection Vulnerabilities

Exploit

cve.report (archive)

text/html

BID 13462

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	Codetosell	Viart Shop Enterprise	2.1.6	All	All	All
Application	Codetosell	Viart Shop Enterprise	2.1.6	All	All	All
cpe:2.3:a:codetosell:viart_shop_enterprise:2.1.6:*:*:*:*:*:						
cpe:2.3:a:codetosell:viart_shop_enterprise:2.1.6:*:*:*:*:*:						

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](#)