



CVE-2004-2411

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2411

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Vp-asp](#) from [Virtual Programming](#) contain the following vulnerability:

The CleanseMessage function in shop\$db.asp for VP-ASP Shopping Cart 4.0 through 5.0 does not sufficiently cleanse inputs, which allows remote attackers to conduct cross-site scripting (XSS) attacks that do not use `<script>` tags, as demonstrated via javascript in IMG tags to (1) the cat parameter in shopdisplayproducts.asp or (2) the msg parameter in shopererror.asp, and possibly other vectors.

CVE-2004-2411 has been assigned by [M](#) 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
Secunia - Advisories - VP-ASP Shopping Cart Cross-Site Scripting Vulnerabilities	Vendor Advisory web.archive.org text/html	X SECUNIA 11846
Neohapsis Archives - Full Disclosure List - #0363 - [Full-Disclosure] VP-ASP Shopping Cart Multiple Vulnerabilities	Exploit Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	FULLDISC 20040613 VP-ASP Shopping Cart Multiple Vulnerabilities
Virtual Programming VP-ASP Shopererror Script Cross-Site Scripting Vulnerability	Exploit Patch cve-report/archive	BID 10534

	cve.report (archive) text/html	
Virtual Programming VP-ASP Shopping Cart Shop\$DB.ASP Cross-Site Scripting Vulnerability	Patch cve.report (archive) text/html	 BID 10530
Provide Security: Advisory - 06142004-01	Exploit Patch Vendor Advisory www.providesecurity.com text/html	 MISC www.providesecurity.com/research/advisories/06142004-01.asp
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 6949
Error Page	Patch web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.vpasp.com/virtprog/info/faq_securityfixes.htm
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF vpassp-shoperror-xss(16411)

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	Virtual Programming	Vp-asp	4.0	All	All	All
Application	Virtual Programming	Vp-asp	4.50	All	All	All
Application	Virtual Programming	Vp-asp	5.0	All	All	All
Application	Virtual Programming	Vp-asp	4.0	All	All	All
Application	Virtual Programming	Vp-asp	4.50	All	All	All
Application	Virtual Programming	Vp-asp	5.0	All	All	All
cpe:2.3:a:virtual_programming:vp-asp:4.0:*:*:*:*:*:						
cpe:2.3:a:virtual_programming:vp-asp:4.50:*:*:*:*:*:						
cpe:2.3:a:virtual_programming:vp-asp:5.0:*:*:*:*:*:						
cpe:2.3:a:virtual_programming:vp-asp:4.0:*:*:*:*:*:						
cpe:2.3:a:virtual_programming:vp-asp:4.50:*:*:*:*:*:						
cpe:2.3:a:virtual_programming:vp-asp:5.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [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](#)