



CVE-2009-3803

Published on: 10/27/2009 12:00:00 AM UTC

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

CVE-2009-3803

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 



Certain versions of [Amiro.cms](#) from [Amirocms](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in Amiro.CMS 5.4.0.0 and earlier allow remote attackers to inject arbitrary web script or HTML via the status_message parameter to (1) /news, (2) /comment, (3) /forum, (4) /blog, and (5) /tags; the status_message parameter to (6) forum.php, (7) discussion.php, (8) guestbook.php, (9) blog.php, (10) news.php, (11) srv_updates.php, (12) srv_backups.php, (13) srv_twist_prevention.php, (14) srv_tags.php, (15) srv_tags_reindex.php, (16) google_sitemap.php, (17) sitemap_history.php, (18) srv_options.php, (19) locales.php and (20) plugins_wizard.php in _admin/; a crafted IMG BBcode tag in the message body of a (21) forum, (22) guestbook, or (23) comment; (24) the content of an avatar file, which is not properly handled by Internet Explorer; and (25) the loginname parameter (aka username) in _admin/index.php.

CVE-2009-3803 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

ONsec.ru тесты на проникновение, исследование безопасности, устранение последствий, аудит информационной безопасности, защиты программ.

Tags

Exploit

web.archive.org

text/html

Inactive Link

Not Archived

Link

ON **MISC** www.onsec.ru/vuln?id=11

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

XF **amiro-loginname-**

	text/html	xss(53893)
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF amiro-statusmessage-xss(53892)
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2009-2967
Files ≈ Packet Storm	Exploit packetstormsecurity.org text/html	 MISC packetstormsecurity.org/0910-exploits/ONSEC-09-004.txt
Amiro.CMS Cross-Site Scripting and Information Disclosure Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 37065

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	Amirocms	Amiro.cms	4.0.8.0	All	All	All
Application	Amirocms	Amiro.cms	4.2.0.5	All	All	All
Application	Amirocms	Amiro.cms	4.2.1.0	All	All	All
Application	Amirocms	Amiro.cms	4.2.2.0	All	All	All
Application	Amirocms	Amiro.cms	4.2.3.0	All	All	All
Application	Amirocms	Amiro.cms	4.2.4	All	All	All
Application	Amirocms	Amiro.cms	4.2.5	All	All	All
Application	Amirocms	Amiro.cms	5.0.7	All	All	All
Application	Amirocms	Amiro.cms	5.2	All	All	All
Application	Amirocms	Amiro.cms	5.2.2	All	All	All
Application	Amirocms	Amiro.cms	5.2.3	All	All	All
Application	Amirocms	Amiro.cms	4.0.8.0	All	All	All
Application	Amirocms	Amiro.cms	4.2.0.5	All	All	All
Application	Amirocms	Amiro.cms	4.2.1.0	All	All	All
Application	Amirocms	Amiro.cms	4.2.2.0	All	All	All
Application	Amirocms	Amiro.cms	4.2.3.0	All	All	All
Application	Amirocms	Amiro.cms	4.2.4	All	All	All
Application	Amirocms	Amiro.cms	4.2.5	All	All	All
Application	Amirocms	Amiro.cms	5.0.7	All	All	All

Application	Amirocms	Amiro.cms	5.2	All	All	All
Application	Amirocms	Amiro.cms	5.2.2	All	All	All
Application	Amirocms	Amiro.cms	5.2.3	All	All	All
Application	Amirocms	Amiro.cms	All	All	All	All
cpe:2.3:a:amirocms:amiro.cms:4.0.8.0:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.2.0.5:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.2.1.0:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.2.2.0:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.2.3.0:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.2.4:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.2.5:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:5.0.7:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:5.2:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:5.2.2:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:5.2.3:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.0.8.0:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.2.0.5:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.2.1.0:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.2.2.0:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.2.3.0:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.2.4:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:4.2.5:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:5.0.7:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:5.2:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:5.2.2:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:5.2.3:*:*:*:*:*:						
cpe:2.3:a:amirocms:amiro.cms:*:*:*:*:*:						

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](#)