PHP Live! Multiple Cross-Site Scripting Vulnerabilities

2006-12-26 17:14:17 by Raven

SECUNIA ADVISORY ID: SA23488

VERIFY ADVISORY: http://secunia.com/advisories/23488/

CRITICAL: Less critical

IMPACT: Cross Site Scripting

SOFTWARE: PHP Live! 3.x - http://secunia.com/product/8575/

DESCRIPTION: Doz has reported some vulnerabilities in PHP Live!, which can be exploited by malicious people to conduct cross-site scripting attacks. The vulnerabilities are reported in version 3.2.2. Other versions may also be affected.

1) Input passed to the "search_string" parameter in setup/transcripts.php is not properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site. Successful exploitation requires that the target user has got administrator credentials.

2) Input passed to the "l" parameter in index.php and the "deptid" and "x" parameters in message_box.php is not properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

SOLUTION: Edit the source code to ensure that input is properly sanitised.

PROVIDED AND/OR DISCOVERED BY: Doz