mxBB Portal mx_tinies Module *module_root_path* File Inclusion

2006-12-04 11:45:33 by Raven

SECUNIA ADVISORY ID: SA23206

VERIFY ADVISORY: http://secunia.com/advisories/23206/

CRITICAL: Highly critical

IMPACT: System access

SOFTWARE: mx_tinies (module for mxBB) 1.x - http://secunia.com/product/12794/

DESCRIPTION: bd0rk has reported a vulnerability in the mx_tinies module for MxBB, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "module_root_path" parameter in includes/common.php is not properly verified before being used to include files. This can be exploited to execute arbitrary PHP code by including files from local or external resources. Successful exploitation requires that "register_globals" is enabled. The vulnerability is reported in version 1.3.0. Other versions may also be affected.

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

PROVIDED AND/OR DISCOVERED BY: bd0rk

ORIGINAL ADVISORY: http://milw0rm.com/exploits/2885