WS_FTP LE *PASV* Response Buffer Overflow Vulnerability

2006-09-25 17:11:42 by Raven

TITLE: WS_FTP LE *PASV* Response Buffer Overflow Vulnerability

SECUNIA ADVISORY ID: SA22032

VERIFY ADVISORY: http://secunia.com/advisories/22032/

CRITICAL: Moderately critical

IMPACT: DoS, System access

WHERE: >From remote

SOFTWARE: WS_FTP LE 5.x - http://secunia.com/product/12062/

DESCRIPTION: h07 has discovered a vulnerability in WS_FTP LE, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error within the handling of responses to the "PASV" command. This can be exploited to cause a buffer overflow by e.g. tricking a user into connecting to a malicious FTP server. Successful exploitation allows execution of arbitrary code. The vulnerability has been confirmed in version 5.08. Other versions may also be affected.

SOLUTION: Connect to trusted FTP servers only. Use another product.

PROVIDED AND/OR DISCOVERED BY: h07

https://www.ravenphpscripts.com/modules.php?name=News&file=article&sid=2407