GuppY *error.php* Cookie Remote Code Execution

2007-01-30 18:19:42 by Raven

SECUNIA ADVISORY ID: SA23914

VERIFY ADVISORY: http://secunia.com/advisories/23914/

CRITICAL: Highly critical

IMPACT: System access

SOFTWARE: GuppY 4.x - http://secunia.com/product/5665/

DESCRIPTION: rgod has discovered two vulnerabilities in GuppY, which can be exploited by malicious people to compromise vulnerable systems. Input passed to the "REMOTE_ADDR" and "msg[x][0]" cookies in error.php is not properly sanitised before being stored in .inc files. This can be exploited to execute arbitrary PHP code by requesting the .inc file through error.php. The vulnerabilities are confirmed in version 4.5.16. Other versions may also be affected.

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

PROVIDED AND/OR DISCOVERED BY: rgod

ORIGINAL ADVISORY: http://milw0rm.com/exploits/3221

https://www.ravenphpscripts.com/modules.php?name=News&file=article&sid=2709