# bit2font vulnerabilities discovery

### 0x1 Introduction

The package **bm2font** accepts graphic input in one of several standard bitmap graphic formats, and converts it to "fonts", each glyph of which covers a tile of the image.

It is a package widley used in texeditor, such as textlive, etc.

https://www.texlive.info/CTAN/graphics/bm2font/

The latest version 3.0 package can be found at:

https://ctan.org/tex-archive/graphics/bm2font

#### **Files**

|    | Name               | Size   | Date       | Notes |
|----|--------------------|--------|------------|-------|
| S. | <u>Gnu.licence</u> | 12 kB  | 1994-02-25 |       |
|    | <u>Makefile</u>    | 926    | 1994-02-25 |       |
|    | Makefile.dos       | 418    | 1994-02-25 |       |
|    | README             | 4 kB   | 1994-02-25 |       |
|    | bm2font-win32.exe  | 75 kB  | 2000-12-25 |       |
|    | bm2font.c          | 111 kB | 1994-10-26 |       |
|    | bm2font.exe        | 77 kB  | 1994-04-29 |       |
|    | loc.p2clib.c       | 124    | 1994-02-25 |       |
|    | manual.zip         | 482 kB | 1993-06-15 |       |
|    | <u>p2c.h</u>       | 13 kB  | 1994-02-25 |       |
| 9  | p2clib.c           | 18 kB  | 1994-02-25 |       |

#### 0x2 Vul1

#### 0x2.1 Crash scene

After executing bm2font with a parameter lentgh over 256(no matter such a file exists), bm2font get crash.

```
This is BitMapTOfont, version 3.0 of january 94, via p2c Converting Bitmap Files to TeX-Fonts
100 200100 5005 5010507215
  #0 0x7febf9e5378e (/usr/lib/x86 64-linux-gnu/libasan.so.2+0x6278e)
  #1 0x405ca9 in main (/home/test/Desktop/evaulation/bm2font/bm2font/bm2font+0
x405ca9)
  #2 0x7febf973e82f in libc start main (/lib/x86 64-linux-gnu/libc.so.6+0x20
82f)
  #3 0x40d1e8 in start (/home/test/Desktop/evaulation/bm2font/bm2font/bm2font
+0x40d1e8)
AddressSanitizer can not describe address in more detail (wild memory access sus
pected).
AddressSanitizer can not describe address in more detail (wild memory access sus
pected).
SUMMARY: AddressSanitizer: strcpy-param-overlap ??:0 ??
==81370==ABORTING
```

#### using gdb to debug:

set breakpoint at 0x405CA5 and go to next instruction.

## 0x2.2 Cause of vulnerability

The main function of bm2font lacks the check of input parameter length. When the first parameter is a character string that does not start with the symbol '-' and has a length greater than 1, it will eventually be copied to the variable **font**.

```
3/33
         printr(
                  -z<area or gradation>
         printf("-m<width of picture on paper>
                                                     (in mm)\n");
3734
         printf("-n<height of picture on paper>
3735
                                                     (in mm)\n");
         printf("-j<clip off white space>
3736
                                                     (y or n, std y)n");
         printf("-k<color: c,m,y or k>
3737
                                                     (std k)\n");
         /*readln(comment);
3738
3739 if length(comment)=0 then goto 9999; j:=ord(comment[0])+1;
3740 if j<=127 then move(comment[0],mem[prefixseg:$80],j);*/
3741
         goto _L9999;
3742
       /*:110*/
3743
3744
       /*111:*/
3745
       for (j = 1; j < P_argc; j++) {</pre>
         strcpy(comment, P_argv[j]);
if (comment[0] != '-') {
3746
3747
3748
           strcpy(font, comment);
           if (strlen(font) < 1 | \|\left(strcmp(font, " ")) {</pre>
3749
3750
             printf("give the name of your bitmap file next time\n");
3751
             goto _L9999;
3752
3753
         } else {
           switch (comment[1]) {
3754
3755
           case 'h':
3756
           case 'H':
3757
3758
             strdelete((Anyptr)comment, 1, 2);
             i = (sscanf(comment, "%lg", &truehres) == 0);
3759
3760
             break;
3761
           case 'v':
3762
```

The **font** will copied to **bmname**. And a crash is triggered when the length of **font** is more than 256.

```
3956
          pheight[j][i] = 0;
3957
          yoffset[j][i] = 0;
3958
3959
3960
     for (i = 0; i <= 128; i++)
3961
       dirpoint[i] = 0;
3962 for (i = 0; i <= 128; i++)
3963
       pkpoint[i] = 0;
3964 for (i = 0; i <= 52; i++)
3965
      charpf[i] = 0;
3966 maxx = 0;
3967
     minx = 646;
3968
     mapheight = 0;
                      /*:108*/
3969
      fok = true;
      strcpy(bmname, font);
3970
3971
      strcpy(bitmap_NAME, bmname);
     if (bitmap != NULL)
3972
        bitmap = freopen(bitmap_NAME, "rb", bitmap);
3973
3974 else
3975
        bitmap = fopen(bitmap_NAME, "rb");
3976
       SETIO(bitmap != NULL, FileNotFound);
      filestat = P_ioresult;
3977
3978
     if (filestat == 0)
3979
       fok = false;
3980 else
       fok = true;
3981
3982 if (fok) {
                   /*113:*/
        printf("File %s not found, abort\n", font);
3983
        filenrohlem().
3001
 94 Static ebts b2[3000];
 95 Static ebts b3[3000];
 96 Static ebts b4[3000];
 97 Static long linepos_, posbit;
 98 Static halfk dbuf;
 99 Static boolean clipon, zeroline, zerorow, nameok, fok;
100 Static Char cmd[256];
101 Static Char bmname[256];
102 Static Char font[256];
103 Static Char tmpname[256];
104 Static Char fontpre[256];a
105 Static Char fontupc[256];
106 Static ebts curpat[2];
```

### 0x2.3 Reproduce

Just run cmd

or run bm2font with a bmp with its path prefix(length of bmp file name is 255))

```
test@ubuntu:~/Desktop/evaulation/bm2font/bm2font$ ./bm2font ../fuzz_test/in/qqqq
qqqqqq.bmp
This is BitMapTOfont, version 3.0 of january 94, via p2c
Converting Bitmap Files to TeX-Fonts
#0 0x7ff99708978e (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x6278e)
  #1 0x405ca9 in main (/home/test/Desktop/evaulation/bm2font/bm2font/bm2font+0
x405ca9)
  #2 0x7ff99697482f in libc start main (/lib/x86 64-linux-gnu/libc.so.6+0x20
  #3 0x40d1e8 in _start (/home/test/Desktop/evaulation/bm2font/bm2font/bm2font
+0x40d1e8)
AddressSanitizer can not describe address in more detail (wild memory access sus
pected).
AddressSanitizer can not describe address in more detail (wild memory access sus
pected).
SUMMARY: AddressSanitizer: strcpy-param-overlap ??:0 ??
==82202==ABORTING
```

#### 0x3 Vul2

#### 0x3.1 Crash scene

After executing bm2font with a parameter start with symbols '-f' with any suffix of length 256 or more, the program goto crash. Note the address santizier reports the different crash location comapre to vul1.

```
test@ubuntu:~/Desktop/evaulation/bm2font/bm2font$ ./bm2font -f11111111111111111111
11
This is BitMapTOfont, version 3.0 of january 94, via p2c
Converting Bitmap Files to TeX-Fonts
GIU.II.CEIICE (OC.DZCIID.C IOC.DZ
  #0 0x7fd06c8ec78e (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x6278e)
  #1 0x4057cf in main (/home/test/Desktop/evaulation/bm2font/bm2font/bm2font+0
x4057cf)
  #2 0x7fduc1d782f in libc start main (/lib/x86 64-linux-gnu/libc.so.6+0x20
  #3 0x40d1e8 in _start (/home/test/Desktop/evaulation/bm2font/bm2font/bm2font
+0x40d1e8)
AddressSanitizer can not describe address in more detail (wild memory access sus
AddressSanitizer can not describe address in more detail (wild memory access sus
SUMMARY: AddressSanitizer: strcpy-param-overlap ??:0 ??
==83133==ABORTING
```

We set a breakpoint around 0x4057cf and step in two instructions.

```
code:x86:64
                                       esi, 0x62c780
edi, 0x62c680
     0x4057c6 <main+2230>
                                mov
     0x4057cb <main+2235>
                                call
                                       0x4012f0 <strcpy@plt>
                                MOV
     0x4057d0 <main+2240>
                                       BYTE PTR [rip+0x226e91], 0x1
                                                                           # 0x62
c668 <aliasused>
                                       0x405403 <main+1267>
     0x4057d7 <main+2247>
                                jmp
     0x4057dc <main+2252>
                                       edx, 0x2
                                MOV
                                                     threads
[#0] Id 1, Name: "bm2font", stopped, reason: BREAKP
[#0] 0x4057c1 \rightarrow matn()
gef≯ si
0x00000000004057c6 in main ()
 Legend:
                                    | Heap | Stack | String ]
```

After executing stcpy() at address 0x4057cb, the bit2font crashed.

```
0x4012f0 <strcpy@plt+0>
                                QWORD PTR [rip+0x22adca]
                                                          # 0x62c
                           jmp
0c0 <strcpy@got.plt>
      0x4012f6 <strcpy@plt+6>
                           push
                                0x15
      0x4012fb <strcpy@plt+11>
                           jmp
                                0x401190
      0x401300 <read@plt+0>
                                QWORD PTR [rip+0x22adc2]
                           jmp
                                                          # 0x62c
0c8 <read@got.plt>
      0x401306 <read@plt+6>
                           push
                                0x16
      0x40130b <read@plt+11>
                           jmp
                                0x401190
                          arguments (guessed)
strcpy@plt (
  11[...]",
  Srdx = 0x00000000000000002
                                        threads
                       reason: SINGLE STEP
[#0] Id 1, Name: "bm2font",
                                          trace
[#0] 0x4057cb → matn()
gef≯ ni
______
#0 0x7ffff6ecc78e (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x6278e)
   #1 0x4057cf in main (/home/test/Desktop/evaulation/bm2font/bm2font/bm2font+0
x4057cf)
   #2 0x7ffff67b782f in libc start main (/lib/x86 64-linux-gnu/libc.so.6+0x20
   #3 0x40d1e8 in _start (/home/test/Desktop/evaulation/bm2font/bm2font/bm2font
+0x40d1e8)
AddressSanitizer can not describe address in more detail (wild memory access sus
AddressSanitizer can not describe address in more detail (wild memory access sus
```

# 0x3.2 Cause of vulnerability

SUMMARY: AddressSanitizer: strcpy-param-overlap ??:0 ??

[Inferior 1 (process 83270) exited with code 01]

pected).

==83270==ABORTING

The program directly copies the first received parameter to the variable **comment** and judge the value of the first and the second characters.

```
3745
      for (j = 1; j < P_argc; j++) {</pre>
3746
        strcpy(comment, P_argv[j]);
        if (comment[0] != '-') {
3747
3748
          strcpy(font, comment);
          if (strlen(font) < 1 || !strcmp(font, " ")) {</pre>
3749
3750
             printf("give the name of your bitmap file next time\n");
3751
            goto _L9999;
3752
3753
        } else {
3754
          switch (comment[1]) { 
3755
          case 'h':
3756
          case 'H':
3757
3758
            strdelete((Anyptr)comment, 1, 2);
             i = (sscanf(comment, "%lg", &truehres) == 0);
3759
3760
            break;
3761
          case 'v':
3762
          case 'V':
3763
            strdelete((Anyptr)comment, 1, 2);
3764
             i = (sscanf(comment, "%lg", &truevres) == 0);
3765
3766
            break;
3767
```

When the first character is '-' and the second character is 'f', it copys the variable **comment** to the **akiasname** after deleting the prefix '-f'.

```
case 'f':
3836
          case 'F':
3837
3838
            strdelete((Anyptr)comment, 1, 2);
            strcpy(aliasname, comment);
3839
3840
             aliasused = true;
3841
            break;
3842
          case 's':
3843
          case 'S':
3844
            strdelete((Anyptr)comment, 1, 2);
3845
             ledprinter = (!strcmp(comment, "y") || !strcmp(comment, "Y"));
3846
3847
            break:
```

If a suffix length of '-f' of 256, it will trigger a stack overflow.

```
132 Static FILE *texfile;
133 Static FILE *bitmap, *pxlfile, *tmpfil;
134 Static short filestat;
135 Static unsigned short gi;
136 Static boolean invert;
137 Static unsigned short cv, dv, lv;
138 Static Char comment[256];
139 Static Char aliasname[256];
140 Static boolean aliasused;
141 Static double mapdiv;
142 Static long pkwidth, pkheight;
143 Static boolean nowhite, halfinch;
144 Static pxlstr nextmemfree;
```

## 0x3.3 Reproduce

Just run cmd

## Note

The causes of above vulnerabilities are orthogonal, they caused stack overflow in different locations.