Bip - Bug #642

Build failure with GCC 9: using a strncpy to copy a single constant byte without NUL termination

2019-01-25 11:03 - Adam Williamson

Status:	New	**Start date:**	2019-01-25
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Patch Available:		**Branch:**	
Found in Versions:		**Security:**	
Confirmed:	No	**Help Needed:**	

Description

So the Red Hat compiler team very kindly pre-checked build of a bunch of Fedora packages with GCC 9 (which will be showing up in Fedora Rawhide soon), and they flagged up two issues in Bip which will cause it to fail to build with GCC 9. This is the first issue.

I'll just paste Jeff Law's explanation here, because he explains it much better than I could:

gcc -DHAVE_CONFIG_H -I. -I./src -Wall -Wextra -Werror -O2 -g -pipe -Wall -Werror=format-security -Wp,-D_FORTIFY_SOURCE=2 -Wp,-D_GLIBCXX_ASSERTIONS -fexceptions -fstack-protector-strong -grecord-gcc-switches -specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -m64 -mtune=generic -fasynchronous-unwind-tables -fstack-clash-protection -fcf-protection -fPIE -Wno-unused-result -Wno-error=format-truncation -c -o src/log.o src/log.c
BUILDSTDERR: In file included from /usr/include/string.h:494,
BUILDSTDERR: from src/connection.h:26,
BUILDSTDERR: from src/irc.h:16,
BUILDSTDERR: from src/log.c:18:
BUILDSTDERR: In function 'strncpy',
BUILDSTDERR: inlined from 'check_dir_r' at src/log.c:87:5:
BUILDSTDERR: /usr/include/bits/string_fortified.h:106:10: error: '__builtin_strncpy' output truncated before terminating nul copying 1 byte from a string of the same length [-Werror=stringop-truncation]
BUILDSTDERR: 106 | return builtinstrncpy_chk (dest, __src, __len, __bos (_dest));
BUILDSTDERR: | ^~~~~~~
BUILDSTDERR: src/log.c: In function 'log_build_filename':
BUILDSTDERR: src/log.c:148:21: warning: '%04d' directive output may be truncated writing between 4 and 11 bytes into a region of size 5 [-Wformat-truncation=]
BUILDSTDERR: 148 | snprintf(year, 5, "%04d", now->tm_year + 1900);
BUILDSTDERR: | ^~~
BUILDSTDERR: src/log.c:148:20: note: directive argument in the range [-2147481748, 2147483647]

BUILDSTDERR: 148 | snprintf(year, 5, "%04d", now->tm_year + 1900);

BUILDSTDERR: | ^~~~~
BUILDSTDERR: In file included from /usr/include/stdio.h:867,
BUILDSTDERR: from src/log.h:17,
BUILDSTDERR: from src/log.c:17:
BUILDSTDERR: /usr/include/bits/stdio2.h:67:10: note: '__builtinsnprintf_chk' output between 5 and 12 bytes into a destination of size 5
BUILDSTDERR: 67 | return builtin_snprintf_chk (s, __n, __USE_FORTIFY_LEVEL - 1,
BUILDSTDERR: | ^~~~~~~
BUILDSTDERR: 68 | __bos (_s), _fmt, __va_arg_pack ());
BUILDSTDERR: | ~~~~~~
BUILDSTDERR: src/log.c:150:22: warning: '%02d' directive output may be truncated writing between 2 and 11 bytes into a region of size 3 [-Wformat-truncation=]
BUILDSTDERR: 150 | snprintf(month, 3, "%02d", now->tm_mon + 1);
BUILDSTDERR: | ^~~
BUILDSTDERR: src/log.c:150:21: note: directive argument in the range [-2147483647, 2147483647]

BUILDSTDERR: 150 | snprintf(month, 3, "%02d", now->tm_mon + 1);

BUILDSTDERR: | ^~~~~
BUILDSTDERR: In file included from /usr/include/stdio.h:867,
BUILDSTDERR: from src/log.h:17,
BUILDSTDERR: from src/log.c:17:
*BUILDSTDERR: /usr/include/bits/stdio2.h:67:10: note: '_builtin*snprintf_chk' output between 3 and 12 bytes into a destination of size 3*
BUILDSTDERR: 67 | return builtin_snprintf_chk (_s, _n, __USE_FORTIFY_LEVEL - 1,
BUILDSTDERR: | ^~~~~~~
BUILDSTDERR: 68 | __bos (_s), __fmt, __va_arg_pack ());
BUILDSTDERR: | ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
BUILDSTDERR: cc1: all warnings being treated as errors
make[1]: Leaving directory '/builddir/build/BUILD/bip-0.9.0-rc3'
RPM build errors:

SO the first error is the easiest to deal with. In check_dir_r we have:

```
while (*tmp == '/') {
                        if (slash_ok) {
                                strncpy(dir + count, "/", 1);
                                count++;
                                slash_ok = 0;
                        }
                        tmp++;
                }
```

Note the code is using a strncpy to copy a single constant byte without NUL termination. That's wasteful and runs afoul of gcc-9's attempts to track when the destination is not going to properly terminated.

Our recommendation is to replace the strncpy call with

dir[count] = '/';

History

#1 - 2019-02-11 23:18 - Adam Williamson

It seems 87192685f55856d2c28021963ab2c308e21faddc is intended to address this, I think? Is that right?

#2 - 2019-02-11 23:45 - Adam Williamson

Yep, it seems to. At least, current git builds fine with GCC 9. Please go ahead and close this.