

Re: Segmentation fault in csh if "setenv LC_ALL C" is sourced

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/stable/2003-12/0199.html>

From: Jordan K. Hubbard (jkh_at_queasyweasel.com)

Date: 12/24/03

Date: Tue, 23 Dec 2003 17:15:12 -0800

To: Mike Tanca <mike@sentex.net>

All,

This should now be fixed. My apologies, again, for the breakage. Please cvsup, re-build your worlds and re-enable your LC_LOCALES as appropriate. :)

– Jordan

On Dec 23, 2003, at 1:23 PM, Mike Tanca wrote:

> At 04:11 PM 23/12/2003, David Wolfskill wrote:
>> This was a rather surprising development this morning.
>
> My guess its related to
>
> *jkh 2003/12/22 12:45:16 PST*
>
> *FreeBSD src repository*
>
> *Modified files: (Branch: RELENG_4)*
> *lib/libc/locale ldpart.c*
> *Log:*
> *MFC: fix memory leak in setlocale() helper functions.*
> *PR#: misc/59910*
>
> *Revision Changes Path*
> *1.7.2.4 +6 -6 src/lib/libc/locale/ldpart.c*
>
>
>
>> I had updated my –STABLE sources per my daily ritual, then did the
>> usual "make buildworld" & friends and rebooted. I logged in (via
>> xdm's
>> login screen, as usual), and got a login screen before I had a chance

freebsd-stable: Re: Segmentation fault in csh if "setenv LC_ALL C" is sourced

```
>> to
>> enter my SSH passphrase. Repeated attempts yielded the same effect.
>>
>> I switched to a vty and logged in ... and was presented with a login
>> prompt immediately. This was also repeatable. :-{
>>
>> I logged in as root -- successfully.
>>
>> I moved aside ~david/.cshrc, and was then able to login as "david".
>>
>> I then tried "source .cshrc.save" and found that csh got a
>> Segmentation
>> fault while processing that directive. Trying various incantations
>> with
>> "csh -x" indicated that there was something about the "setenv LC_ALL
>> C"
>> line in my ~/.cshrc that it didn't like at all, so I created a new
>> ~/.cshrc like the old one, but without that line (and the one before
>> it); csh seemed to cope with that OK.
>>
>> So here's the result from what debugging I've done so far. I confess
>> that I'm fairly rusty with gdb, but I'm willing to poke around:
>>
>> Script started on Tue Dec 23 12:25:20 2003
>> localhost(4.9-S)[1] uname -a
>> FreeBSD localhost 4.9-STABLE FreeBSD 4.9-STABLE #24: Tue Dec 23
>> 06:23:02 PST 2003
>> root@d146.catwhisker.org:/common/S1/obj/usr/src/sys/LAPTOP_30W i386
>> localhost(4.9-S)[2] diff -u .cshrc.save .cshrc
>> --- .cshrc.save Thu Sep 18 05:56:33 2003
>> +++ .cshrc Tue Dec 23 06:39:14 2003
>> @@ -125,8 +125,8 @@
>> setenv PAGER less
>> setenv RNINIT ~/.rninit
>> setenv FTP_PASSIVE_MODE
>> -setenv LANG en_US.ISO8859-1
>> -setenv LC_ALL C
>> +# setenv LANG en_US.ISO8859-1
>> +# setenv LC_ALL C
>> unset autologout
>> set history = 900
>> unset noclobber
>> localhost(4.9-S)[3] csh -x
>> localhost(4.9-S)[1] source .cshrc.save
>> source .cshrc.save
>> set npath =
>> if ( 1 ) then
>> set dir = ~/bin/FreeBSD
>> if ( -d /home/david/bin/FreeBSD ) then
>> true
>> else
```

freebsd-stable: Re: Segmentation fault in csh if "setenv LC_ALL C" is sourced

```
>> else
>> if ( 1 ) then
>> if { test -n /home/david/bin/FreeBSD } then
>> test -n /home/david/bin/FreeBSD
>> if ( -d /home/david/bin/FreeBSD ) then
>> set npath = /home/david/bin/FreeBSD
>> endif
>> endif
>> endif
>> setenv SYMONHOME /opt/SUNWsymon
>> set path = ( /home/david/bin/FreeBSD ~/bin /bin /usr/bin /sbin
>> /usr/sbin /usr/local/sbin /usr/local/bin /usr/local/pbm
>> /usr/local/rdb /usr/local/bin/mh /usr/share/bin /usr/ucb
>> /usr/local/games /usr/games /usr/X11R6/bin /usr/local/etc /usr/etc
>> /etc /usr/local/office52/program )
>> set HOST = `hostname | sed -e 's/\..*$/''`
>> hostname
>> sed -e s/\..*$/
>> if ( ! 0 ) then
>> if ( 1 != 0 ) then
>> if { test -z %m(4.9-S)[%h] } exit
>> test -z %m(4.9-S)[%h]
>> set u = `uname -r`
>> uname -r
>> set ul = `echo ${u} | sed -e 's/-.*$/''`
>> sed -e s/-.*$/
>> echo 4.9-STABLE
>> set ur = `echo ${u} | sed -e 's/^[^-]*-/'`
>> sed -e s/^[^-]*-//
>> echo 4.9-STABLE
>> switch ( STABLE )
>> set ur = -S
>> breaksw
>> set u = 4.9-S
>> if ( ! 1 ) then
>> set prompt = %m(4.9-S)[%h]
>> endif
>> switch ( FreeBSD )
>> setenv XAPPLRESDIR /usr/X11R6/lib/X11/app-defaults
>> setenv LD_LIBRARY_PATH /usr/lib:/usr/local/X11/lib:/usr/local/lib
>> setenv MY_WM tvtwm
>> setenv MANPATH
>> ~/man:/usr/local/man:/usr/share/man:/usr/X11R6/man:/usr/local/lib/
>> perl5/5.6.0/man:/usr/share/perl/man:/usr/local/lib/perl5/5.00503/man:
>> /usr/local/games/man:/usr/local/lib/perl5/5.6.1/man
>> breaksw
>> endif
>> if ( 0 ) exit
>> setenv GROFF_TMAC_PATH /usr/local/tmac.:/usr/share/groff/tmac
>> setenv ADDRPATH /home/david/addr:/home/david/addr/business
>> setenv PRINTER lp
```

freebsd-stable: Re: Segmentation fault in csh if "setenv LC_ALL C" is sourced

```
>> setenv LPDEST lp
>> setenv EDITOR vi
>> setenv LESS -sMci
>> setenv CVSROOT /cvs
>> setenv HOSTALIASES ~/.hostaliases
>> setenv BLOCKSIZE 1k
>> setenv NNTPSERVER news.sf.sbcglobal.net
>> setenv MM_NOASK image/*
>> setenv PAGER less
>> setenv RNINIT ~/.rninit
>> setenv FTP_PASSIVE_MODE
>> setenv LANG en_US.ISO8859-1
>> Segmentation fault (core dumped)
>> localhost(4.9-S)[4] echo "I built a debug csh in
>> /usr/obj/usr/src/bin/csh"
>> I built a debug csh in /usr/obj/usr/src/bin/csh
>> localhost(4.9-S)[5] /usr/obj/usr/src/bin/csh/csh -x
>> localhost(4.9-S)[1] source .cshrc.save
>> source .cshrc.save
>> [very similar output to the above elided -- dhw]
>> ...
>> setenv LANG en_US.ISO8859-1
>> Segmentation fault (core dumped)
>> localhost(4.9-S)[6] ^Dexit
>>
>> Script done on Tue Dec 23 12:57:51 2003
>>
>> OK; here's what gdb said (via cut'n'paste):
>>
>> localhost(4.9-S)[17] gdb /usr/obj/usr/src/bin/csh/csh csh.core
>> GNU gdb 4.18 (FreeBSD)
>> Copyright 1998 Free Software Foundation, Inc.
>> GDB is free software, covered by the GNU General Public License, and
>> you are
>> welcome to change it and/or distribute copies of it under certain
>> conditions.
>> Type "show copying" to see the conditions.
>> There is absolutely no warranty for GDB. Type "show warranty" for
>> details.
>> This GDB was configured as "i386-unknown-freebsd"...Deprecated
>> bfd_read called a
>> t
>> /usr/src/gnu/usr.bin/binutils/gdb/../../../../contrib/gdb/gdb/
>> dbxread.c line 2
>> 627 in elfstab_build_psymtabs
>> Deprecated bfd_read called at
>> /usr/src/gnu/usr.bin/binutils/gdb/../../../../cont
>> rib/gdb/gdb/dbxread.c line 933 in fill_symbuf
>>
>> Core was generated by `csh'.
>> Program terminated with signal 11, Segmentation fault.
```

Re: Segmentation fault in csh if "setenv LC_ALL C" is sourced

freebsd-stable: Re: Segmentation fault in csh if "setenv LC_ALL C" is sourced

```
>> #0 0x80ad21f in __part_load_locale ()
>> (gdb) bt
>> #0 0x80ad21f in __part_load_locale ()
>> #1 0x80ad0bf in __monetary_load_locale ()
>> #2 0x8090296 in setlocale ()
>> #3 0x808fffc in setlocale ()
>> #4 0x8055fa5 in dosetenv (v=0x812fc40, c=0x8138e00)
>> at /usr/src/bin/csh/../../contrib/tcsh/sh.func.c:1358
>> #5 0x80545dc in func (t=0x8138e00, bp=0x80df1f8)
>> at /usr/src/bin/csh/../../contrib/tcsh/sh.func.c:145
>> #6 0x8061ca7 in execute (t=0x8138e00, wanttty=1210, pipein=0x0,
>> pipeout=0x0,
>> do_glob=1) at /usr/src/bin/csh/../../contrib/tcsh/sh.sem.c:654
>> #7 0x8061f30 in execute (t=0x8132da0, wanttty=1210, pipein=0x0,
>> pipeout=0x0,
>> do_glob=1) at /usr/src/bin/csh/../../contrib/tcsh/sh.sem.c:731
>> #8 0x804aab8 in process (catch=0)
>> at /usr/src/bin/csh/../../contrib/tcsh/sh.c:2159
>> #9 0x804a349 in srcunit (unit=3, onlyown=0, hflg=0, av=0x812fde8)
>> at /usr/src/bin/csh/../../contrib/tcsh/sh.c:1691
>> #10 0x8049d62 in srcfile (f=0xbfbfa130 ".cshrc.save", onlyown=0,
>> flag=0,
>> av=0x812fde8) at /usr/src/bin/csh/../../contrib/tcsh/sh.c:1470
>> #11 0x804ad63 in dosource (t=0x812fde0, c=0x815d3a0)
>> at /usr/src/bin/csh/../../contrib/tcsh/sh.c:2205
>> #12 0x80545dc in func (t=0x815d3a0, bp=0x80df238)
>> at /usr/src/bin/csh/../../contrib/tcsh/sh.func.c:145
>> #13 0x8061ca7 in execute (t=0x815d3a0, wanttty=1210, pipein=0x0,
>> pipeout=0x0,
>> ---Type <return> to continue, or q <return> to quit---
>> do_glob=1) at /usr/src/bin/csh/../../contrib/tcsh/sh.sem.c:654
>> #14 0x8061f30 in execute (t=0x815d380, wanttty=1210, pipein=0x0,
>> pipeout=0x0,
>> do_glob=1) at /usr/src/bin/csh/../../contrib/tcsh/sh.sem.c:731
>> #15 0x804aab8 in process (catch=1)
>> at /usr/src/bin/csh/../../contrib/tcsh/sh.c:2159
>> #16 0x8049b07 in main (argc=0, argv=0xbfbff53c)
>> at /usr/src/bin/csh/../../contrib/tcsh/sh.c:1341
>> (gdb) frame 4
>> #4 0x8055fa5 in dosetenv (v=0x812fc40, c=0x8138e00)
>> at /usr/src/bin/csh/../../contrib/tcsh/sh.func.c:1358
>> 1358 (void) setlocale(LC_ALL, "");
>> (gdb) p dont_free
>> $1 = 0
>> (gdb) p k
>> $2 = 135461960
>> (gdb) frame 3
>> #3 0x808fffc in setlocale ()
>> (gdb)
>>
>>
```

freebsd-stable: Re: Segmentation fault in csh if "setenv LC_ALL C" is sourced

>> *And looking at the man page for setlocale(), I don't see anything*
>> *special*
>> *regarding the second argument being a string of length 0.*
>>
>> *I note further that along with tracking -STABLE on a daily basis,*
>> *I've also been tracking -CURRENT on a daily basis on the same*
>> *machine, using the same home directory (and thus, the same .cshrc).*
>> *And*
>> *I never saw this issue pop up on -CURRENT.*
>>
>> *Am I the only one to see this? Am I doing something wrong (or at*
>> *least,*
>> *unsupported)?*
>>
>> *Thanks in advance for clues!*
>>
>> *Peace,*
>> *david*
>> --
>> *David H. Wolfskill david@catwhisker.org*
>> *If you want true virus-protection for your PC, install a*
>> *non-Microsoft OS*
>> *on it. Plausible candidates include FreeBSD, Linux, NetBSD, OpenBSD,*
>> *and*
>> *Solaris (in alphabetical order).*
>>

>> *freebsd-stable@freebsd.org mailing list*
>> *<http://lists.freebsd.org/mailman/listinfo/freebsd-stable>*
>> *To unsubscribe, send any mail to*
>> *"freebsd-stable-unsubscribe@freebsd.org"*
>
>

--
Jordan K. Hubbard
Engineering Manager, BSD technology group
Apple Computer