Backport192 - Backport #5075

invalid *fdp in Mac OS X and FreeBSD over recvmsg with SCM_RIGHTS

07/22/2011 05:51 PM - naruse (Yui NARUSE)

Status:	Rejected	
Priority:	Normal	
Assignee:	yugui (Yuki Sonoda)	

Description

Mac OS X と FreeBSD にて、存在しない fd を close してしまう問題について、
現在 r32598 で応急処置が施されていますが、根本的な原因について、
sys/kern/uipc_socket.c を見るに、
http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/kern/uipc_socket.c?rev=1.340.2.6.2.1;content-type=text%2Fplain;only_with_tag=RELENG_8_2_0_RELEASE

```
 * Process one or more MT_CONTROL mbufs present before any data mbufs
 * in the first mbuf chain on the socket buffer.  If MSG_PEEK, we
 * just copy the data; if !MSG_PEEK, we call into the protocol to
 * perform externalization (or freeing if controlp == NULL).
```

とあるので、recvmsg に MSG_PEEK を与えた場合は invalid なものが返ってくると思うのですが。

ちなみに、以下のような printf パッチをあてて走らせると、discard_cmsg() に来たものは全て invalid になっています。

diff --git a/ext/socket/ancdata.c b/ext/socket/ancdata.c
index 61e0576..ad44fb4 100644
--- a/ext/socket/ancdata.c
+++ b/ext/socket/ancdata.c
@@ -1379,6 +1379,7 @@ rb_recvmsg(int fd, struct msghdr *msg, int flags)
static void
discard_cmsg(struct cmsghdr *cmh, char *msg_end)
{

- fprintf(stderr, "discard_cmsg-begin\n"); if (cmh->cmsg_level == SOL_SOCKET && cmh->cmsg_type == SCM_RIGHTS) { int *fdp = (int *)CMSG_DATA(cmh); int *end = (int *)((char *)cmh + cmh->cmsg_len); @@ -1391,12 +1392,18 @@ discard_cmsg(struct cmsghdr *cmh, char *msg_end) */ struct stat buf; if (fstat(*fdp, &buf) == 0) {
- fprintf(stderr, "fdp: %d is valid (%p %p %p)\n", *fdp,fdp,end,msg_end); rb_update_max_fd(*fdp); close(*fdp);
  }
- else {
- fprintf(stderr, "fdp: %d is invalid (%p %p %p)\n", *fdp,fdp,end,msg_end);
- rb_backtrace();
- } fdp++; } }
- fprintf(stderr, "discard_cmsg-end\n"); } #endif

@@ -1432,6 +1439,7 @@ make_io_for_unix_rights(VALUE ctl, struct cmsghdr *cmh, char *msg_end)
(char *)fdp + sizeof(int) <= msg_end) {
int fd = *fdp;
struct stat stbuf;

- fprintf(stderr,"makeiounixr: %d (%p %p %p)\n", *fdp,fdp,end,msg_end); VALUE io; if (fstat(fd, &stbuf) == -1)
  rb_raise(rb_eSocket, "invalid fd in SCM_RIGHTS");

History

#1 - 07/22/2011 09:30 PM - kosaki (Motohiro KOSAKI)

xnu/bsd/kern/uipc_socket.c に全く同じコメントがあるので、FreeBSD由来のコードで同じ問題にあたってるんじゃないですかね。

#2 - 07/23/2011 01:47 AM - akr (Akira Tanaka)

- File recvmsg-msg_peek-freebsd.patch added

#3 - 07/23/2011 01:53 AM - akr (Akira Tanaka)

- ruby -v changed from ruby 1.9.4dev (2011-07-22 trunk 32604) [x86_64-freebsd8.2] to -

2011/7/22 Yui NARUSE naruse@airemix.jp:

> Mac OS X と FreeBSD にて、存在しない fd を close してしまう問題について、
> 現在 r32598 で応急処置が施されていますが、根本的な原因について、
> sys/kern/uipc_socket.c を見るに、
> http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/kern/uipc_socket.c?rev=1.340.2.6.2.1;content-type=text%2Fplain;only_with_tag=RELENG_8_2_0_RELEASE
>
> ```
>     * Process one or more MT_CONTROL mbufs present before any data mbufs
>     * in the first mbuf chain on the socket buffer.  If MSG_PEEK, we
>     * just copy the data; if !MSG_PEEK, we call into the protocol to
>     * perform externalization (or freeing if controlp == NULL).
> ```
>
> とあるので、recvmsg に MSG_PEEK を与えた場合は invalid なものが返ってくると思うのですが。

おぉ、素晴らしい。

ではとりあえず FreeBSD と MacOS X で MSG_PEEK のとき、という条件ですかね。
--
[田中 哲][たなか あきら][Tanaka Akira]

#4 - 07/23/2011 01:53 AM - akr (Akira Tanaka)

2011/7/22 Yui NARUSE naruse@airemix.jp:

> Mac OS X と FreeBSD にて、存在しない fd を close してしまう問題について、
> 現在 r32598 で応急処置が施されていますが、根本的な原因について、
> sys/kern/uipc_socket.c を見るに、
> http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/kern/uipc_socket.c?rev=1.340.2.6.2.1;content-type=text%2Fplain;only_with_tag=RELENG_8_2_0_RELEASE
>
> ```
>     * Process one or more MT_CONTROL mbufs present before any data mbufs
>     * in the first mbuf chain on the socket buffer.  If MSG_PEEK, we
>     * just copy the data; if !MSG_PEEK, we call into the protocol to
>     * perform externalization (or freeing if controlp == NULL).
> ```
>
> とあるので、recvmsg に MSG_PEEK を与えた場合は invalid なものが返ってくると思うのですが。

おぉ、素晴らしい。

ではとりあえず FreeBSD と MacOS X で MSG_PEEK のとき、という条件ですかね。
--
[田中 哲][たなか あきら][Tanaka Akira]

#5 - 07/23/2011 08:53 AM - kosaki (Motohiro KOSAKI)

> Issue #5075 has been updated by Akira Tanaka.
>
> File recvmsg-msg_peek-freebsd.patch added

わたしのOS X (Lion)は他のバグでテスト環境として不適切なのでFreeBSD環境の
人にテストお願いしたい。

あと、以前のメールで明確に書けていませんでしたが私が確認したのはSnow Leopardの
ソースなので、誰かが Snow Leopard以前でこの問題が発生しないことが確認しているなら
わたしがコードを誤読しています。コメント中に "Lion" と明記してあるので気になっています。

#6 - 07/23/2011 08:53 AM - kosaki (Motohiro KOSAKI)

> Issue #5075 has been updated by Akira Tanaka.
>
> File recvmsg-msg_peek-freebsd.patch added

わたしのOS X (Lion)は他のバグでテスト環境として不適切なのでFreeBSD環境の
人にテストお願いしたい。

あと、以前のメールで明確に書けていませんでしたが私が確認したのはSnow Leopardの

ソースなので、誰かが Snow Leopard以前でこの問題が発生しないことが確認しているなら
わたしがコードを誤読しています。コメント中に "Lion" と明記してあるので気になっています。

#7 - 07/23/2011 08:59 AM - akr (Akira Tanaka)

2011年7月23日8:40 KOSAKI Motohiro kosaki.motohiro@gmail.com:

> あと、以前のメールで明確に書けていませんでしたが私が確認したのはSnow Leopardの
> ソースなので、誰かが Snow Leopard以前でこの問題が発生しないことが確認しているなら
> わたしがコードを誤読しています。コメント中に "Lion" と明記してあるので気になっています。

そこはたしかに書き方を迷いました。
MacOS X Lion で問題を確認したのは nagachika さんです。

いまのところ誰も MacOS X Snow Leopard 以前での動作確認はしていないと思います。
(興味がある人がいたらなるせさんが提示したパッチを当てて test-all して、invalid が出てくるか
確認してみてください。)
--
[田中 哲][たなか あきら][Tanaka Akira]

#8 - 07/23/2011 08:59 AM - akr (Akira Tanaka)

2011年7月23日8:40 KOSAKI Motohiro kosaki.motohiro@gmail.com:

> あと、以前のメールで明確に書けていませんでしたが私が確認したのはSnow Leopardの
> ソースなので、誰かが Snow Leopard以前でこの問題が発生しないことが確認しているなら
> わたしがコードを誤読しています。コメント中に "Lion" と明記してあるので気になっています。

そこはたしかに書き方を迷いました。
MacOS X Lion で問題を確認したのは nagachika さんです。

いまのところ誰も MacOS X Snow Leopard 以前での動作確認はしていないと思います。
(興味がある人がいたらなるせさんが提示したパッチを当てて test-all して、invalid が出てくるか
確認してみてください。)
--
[田中 哲][たなか あきら][Tanaka Akira]

#9 - 07/23/2011 09:29 AM - taca (Takahiro Kambe)

In message CANjopZGqKbM4O6vMkOHrZcD1YLLOJ86-hDHsK3C+px9kdrW4Eg@mail.gmail.com
on Sat, 23 Jul 2011 01:37:35 +0900,
Tanaka Akira akr@fsij.org wrote:

> Mac OS X と FreeBSD にて、存在しない fd を close してしまう問題について、
> 現在 r32598 で応急処置が施されていますが、根本的な原因について、
> sys/kern/uipc_socket.c を見るに、
> http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/kern/uipc_socket.c?rev=1.340.2.6.2.1;content-type=text%2Fplain;only_with_tag=RELENG_8_2_0_RELEASE
>
> ```
>     * Process one or more MT_CONTROL mbufs present before any data mbufs
>     * in the first mbuf chain on the socket buffer.  If MSG_PEEK, we
>     * just copy the data; if !MSG_PEEK, we call into the protocol to
>     * perform externalization (or freeing if controlp == NULL).
> ```
>
> とあるので、recvmsg に MSG_PEEK を与えた場合は invalid なものが返ってくると思うのですが。

おぉ、素晴らしい。
このコメントは NetBSD current にもあります。FreeBSDから2008年4月14日に
取り込まれていて、リリースでは NetBSD 5には含まれています。

以上、just FYI.

--
神戸 隆博 / Takahiro Kambe

#10 - 07/23/2011 09:29 AM - taca (Takahiro Kambe)

In message CANjopZGqKbM4O6vMkOHrZcD1YLLOJ86-hDHsK3C+px9kdrW4Eg@mail.gmail.com
on Sat, 23 Jul 2011 01:37:35 +0900,
Tanaka Akira akr@fsij.org wrote:

> > Mac OS X [illegible] FreeBSD [illegible] fd [illegible] close [illegible]
> > [illegible] r32598 [illegible]
> > sys/kern/uipc_socket.c [illegible]
> > http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/kern/uipc_socket.c?rev=1.340.2.6.2.1;content-type=text%2Fplain;only_with_tag=RELENG_8_2_0_RELEASE
> >
> > ```
> >      * Process one or more MT_CONTROL mbufs present before any data mbufs
> >      * in the first mbuf chain on the socket buffer.  If MSG_PEEK, we
> >      * just copy the data; if !MSG_PEEK, we call into the protocol to
> >      * perform externalization (or freeing if controlp == NULL).
> > ```
> >
> > [illegible]recvmsg [illegible] MSG_PEEK [illegible] invalid [illegible]
>
> [illegible]
> [illegible] NetBSD current [illegible]FreeBSD[illegible]2008[illegible]4[illegible]14[illegible]
> [illegible] NetBSD 5[illegible]

[illegible]just FYI.

--
[illegible] / Takahiro Kambe

#11 - 07/23/2011 09:59 AM - akr (Akira Tanaka)

2011[illegible]7[illegible]23[illegible]9:26 Takahiro Kambe taca@back-street.net:

> [illegible] NetBSD current [illegible]FreeBSD[illegible]2008[illegible]4[illegible]14[illegible]
> [illegible] NetBSD 5[illegible]

[illegible] defined(**NetBSD**) [illegible]
[illegible]

[illegible]
[illegible]
fd [illegible]-1 [illegible]
([illegible] -1 [illegible])
--
[[illegible]][[illegible]][Tanaka Akira]

#12 - 07/23/2011 09:59 AM - akr (Akira Tanaka)

2011[illegible]7[illegible]23[illegible]9:26 Takahiro Kambe taca@back-street.net:

> [illegible] NetBSD current [illegible]FreeBSD[illegible]2008[illegible]4[illegible]14[illegible]
> [illegible] NetBSD 5[illegible]

[illegible] defined(**NetBSD**) [illegible]
[illegible]

[illegible]
[illegible]
fd [illegible]-1 [illegible]
([illegible] -1 [illegible])
--
[[illegible]][[illegible]][Tanaka Akira]

#13 - 07/23/2011 10:23 AM - kosaki (Motohiro KOSAKI)

> [illegible] defined(**NetBSD**) [illegible]
> [illegible]
>
> [illegible]
> [illegible]
> fd [illegible]-1 [illegible]
> ([illegible] -1 [illegible])

[illegible] configure[illegible]
[illegible]

確認する気になれないけど Dragonflyとかもきっと同じ挙動を示すと思いますし

#14 - 07/23/2011 10:23 AM - kosaki (Motohiro KOSAKI)

> では条件に defined(**NetBSD**) もつけるということで。
> コンパイル時にテストしたい気もしますが。
>
> 本当は、カーネルはコンパイル時とは変わることもあるし、
> 動的に検査できるといいんですが。
> fd を返さないときには、-1 にしてくれればいいのに。
> (もしかして、事前にバッファを -1 で埋め尽くしておけばいい?)

今のところバージョン依存の要素は薄そうなので configureで判定してしまって
いいのではないでしょうか。
確認する気になれないけど Dragonflyとかもきっと同じ挙動を示すと思いますし

#15 - 07/23/2011 02:48 PM - nagachika (Tomoyuki Chikanaga)

わたしが確認したのは Snow Leopard でした。MSG_PEEK をつけた recvmsg() で不正な fd が取り出されるのを確認しました。

#16 - 07/24/2011 06:10 PM - akr (Akira Tanaka)

- Status changed from Assigned to Closed

コンパイル時に挙動を検査するようにしました。

これで close とします。

#17 - 07/24/2011 11:22 PM - akr (Akira Tanaka)

- File 5075-1.9.2.patch added

- Status changed from Closed to Assigned

- Assignee changed from akr (Akira Tanaka) to yugui (Yuki Sonoda)

- Target version changed from 1.9.3 to 1.9.2

1.9.2 用のパッチを作ったので添付します。

#18 - 07/25/2011 03:32 AM - naruse (Yui NARUSE)

- Tracker changed from Bug to Backport

- Project changed from Ruby master to Backport192

- Category changed from ext to ext

- Target version deleted (1.9.2)

#19 - 05/30/2016 08:33 AM - naruse (Yui NARUSE)

- Status changed from Assigned to Rejected

Files

recvmsg-msg_peek-freebsd.patch	4.71 KB	07/23/2011	akr (Akira Tanaka)
5075-1.9.2.patch	23.2 KB	07/24/2011	akr (Akira Tanaka)