

git index : openssh.git

Portable OpenSSH

master summary refs log tree **commit** difflog msg

author markus@openbsd.org <markus@openbsd.org> 2016-09-19 19:02:19 +0000
 committer Damien Miller <djm@mindrot.org> 2016-09-21 11:03:55 +1000
 commit 28652bca29046f62c7045e933e6b931de1d16737 (patch)
 tree 54780f2ea3a511e4b80b9888b0fa20e71418f09e
 parent 492710894acfcc2f173d14d1d45bd2e688df605d (diff)

diff options

context:
 space:
 mode:

upstream commit

move inbound NEWKEYS handling to kex layer; otherwise early NEWKEYS causes NULL deref; found by Robert Swiecki/honggfuzz; fixed with & ok djm@

Upstream-ID: 9a68b882892e9f51dc7bfa9f5a423858af358b2f

Diffstat

```
-rw-r--r-- kex.c 4   

-rw-r--r-- packet.c 6 
```

2 files changed, 5 insertions, 5 deletions

diff --git a/kex.c b/kex.c**index f4c130f14..8800d4001 100644****--- a/kex.c****+++ b/kex.c****@@ -1,4 +1,4 @@****/* \$OpenBSD: kex.c,v 1.121 2016/09/12 23:31:27 djm Exp \$ */****+/* \$OpenBSD: kex.c,v 1.122 2016/09/19 19:02:19 markus Exp \$ */**

/*

* Copyright (c) 2000, 2001 Markus Friedl. All rights reserved.

*
@@ -425,6 +425,8 @@ kex_input_newkeys(int type, u_int32_t seq, void *ctxt)ssh_dispatch_set(ssh, SSH2_MSG_NEWKEYS, &kex_protocol_error);
 if ((r = sshpkt_get_end(ssh)) != 0)

return r;

+ if ((r = ssh_set_newkeys(ssh, MODE_IN)) != 0)**+ return r;**

kex->done = 1;

sshbuf_reset(kex->peer);

/* sshbuf_reset(kex->my); */

diff --git a/packet.c b/packet.c**index 711091da7..fb316acbc 100644****--- a/packet.c****+++ b/packet.c****@@ -1,4 +1,4 @@****/* \$OpenBSD: packet.c,v 1.237 2016/09/12 01:22:38 deraadt Exp \$ */****+/* \$OpenBSD: packet.c,v 1.238 2016/09/19 19:02:19 markus Exp \$ */**

/*

* Author: Tatu Ylonen <ylo@cs.hut.fi>

* Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland

@@ -1907,9 +1907,7 @@ ssh_packet_read_poll2(struct ssh *ssh, u_char *typep, u_int32_t *seqnr_p)

return r;

return SSH_ERR_PROTOCOL_ERROR;

}
- if (*typep == SSH2_MSG_NEWKEYS)**- r = ssh_set_newkeys(ssh, MODE_IN);****- else if (*typep == SSH2_MSG_USERAUTH_SUCCESS && !state->server_side)**

```
+ if (*typep == SSH2_MSG_USERAUTH_SUCCESS && !state->server_side)
    r = ssh_packet_enable_delayed_compress(ssh);
else
    r = 0;
```

generated by cgit v1.2.3 (git 2.25.1) at 2026-05-02 18:04:44 +0000