

untrusted comment: signature from openbsd 6.0 base secret key  
 RWSho3oKSqgLQ+nvjojNv0BETtBpd0sfAjnPnz8Ko3XL5UcaGDRRrkHt9GulGnU/URXBZxe3q32a0gGie01P3mF9iSo0  
 umkskAQ=

OpenBSD 6.0 errata 13, Oct 10, 2016:

A protocol parsing bug in sshd can lead to unauthenticated memory  
 and CPU consumption.

Apply by doing:

```
signify -Vep /etc/signify/openbsd-60-base.pub -x 013_ssh_kexinit.patch.sig \  

  -m - | (cd /usr/src && patch -p0)
```

And then rebuild and install sshd:

```
cd /usr/src/usr.bin/ssh  

make obj  

make depend  

make  

make install
```

Index: usr.bin/ssh/kex.c

```
=====
RCS file: /cvs/src/usr.bin/ssh/kex.c,v
retrieving revision 1.118
retrieving revision 1.118.4.1
diff -p -u -IopenBSD -r1.118 -r1.118.4.1
--- usr.bin/ssh/kex.c      2 May 2016 10:26:04 -0000      1.118
+++ usr.bin/ssh/kex.c     10 Oct 2016 19:35:47 -0000      1.118.4.1
@@ -452,6 +452,7 @@ kex_input_kexinit(int type, u_int32_t se
     if (kex == NULL)
         return SSH_ERR_INVALID_ARGUMENT;

+    ssh_dispatch_set(ssh, SSH2_MSG_KEXINIT, NULL);
     ptr = sshpkt_ptr(ssh, &dlen);
     if ((r = sshbuf_put(kex->peer, ptr, dlen)) != 0)
         return r;
```