CVE-2017-6542

描述：The ssh\_agent\_channel\_data function in PuTTY before 0.68 allows remote attackers to have unspecified impact via a large length value in an agent protocol message and leveraging the ability to connect to the Unix-domain socket representing the forwarded agent connection, which trigger a buffer overflow.

软件：PuTTY

源码：ssh.c

出现位置： 5697-5736行

关键源码：

static int ssh\_agent\_channel\_data(struct ssh\_channel \*c, char \*data,

int length)

{

while (length > 0) {

if (c->u.a.lensofar < 4) {

unsigned int l = min(4 - c->u.a.lensofar, (unsigned)length);

memcpy(c->u.a.msglen + c->u.a.lensofar, data, l);

data += l;

length -= l;

c->u.a.lensofar += l;

}

if (c->u.a.lensofar == 4) {

c->u.a.totallen = 4 + GET\_32BIT(c->u.a.msglen);

c->u.a.message = snewn(c->u.a.totallen, unsigned char);

memcpy(c->u.a.message, c->u.a.msglen, 4);

}

if (c->u.a.lensofar >= 4 && length > 0) {

unsigned int l = min(c->u.a.totallen - c->u.a.lensofar,

(unsigned)length);

memcpy(c->u.a.message + c->u.a.lensofar, data, l);

data += l;

length -= l;

c->u.a.lensofar += l;

}

if (c->u.a.lensofar == c->u.a.totallen) {

void \*reply;

int replylen;

c->u.a.outstanding\_requests++;

c->u.a.pending = agent\_query(

c->u.a.message, c->u.a.totallen, &reply, &replylen,

ssh\_agentf\_callback, c);

if (!c->u.a.pending)

ssh\_agentf\_callback(c, reply, replylen);

sfree(c->u.a.message);

c->u.a.message = NULL;

c->u.a.lensofar = 0;

}

}

return 0; /\* agent channels never back up \*/

}