CVE-2017-7869

描述：GnuTLS before 2017-02-20 has an out-of-bounds write caused by an integer overflow and heap-based buffer overflow related to the cdk\_pkt\_read function in opencdk/read-packet.c. This issue (which is a subset of the vendor's GNUTLS-SA-2017-3 report) is fixed in 3.5.10.

软件：GnuTLS before 2017-02-20

源码：lib/opencdk/read-packet.c

出现位置： 783-790行

关键源码：

else

read\_old\_length(inp, ctb, &pktlen, &pktsize);

+ /\* enforce limits to ensure that the following calculations

+ \* do not overflow \*/

+ if (pktlen >= MAX\_PACKET\_LEN || pktsize >= MAX\_PACKET\_LEN) {

+ \_cdk\_log\_info("cdk\_pkt\_read: too long packet\n");

+ return gnutls\_assert\_val(CDK\_Inv\_Packet);

+ }

pkt->pkttype = pkttype;

pkt->pktlen = pktlen;

pkt->pktsize = pktsize + pktlen;

pkt->old\_ctb = is\_newctb ? 0 : 1; 无边界检查

case CDK\_PKT\_ATTRIBUTE:

#define NAME\_SIZE (pkt->pktlen + 16 + 1)

pkt->pkt.user\_id = cdk\_calloc(1, sizeof \*pkt->pkt.user\_id

+ NAME\_SIZE);

if (!pkt->pkt.user\_id)

return gnutls\_assert\_val(CDK\_Out\_Of\_Core);

pkt->pkt.user\_id->name =

(char \*) pkt->pkt.user\_id + sizeof(\*pkt->pkt.user\_id);

rc = read\_attribute(inp, pktlen, pkt->pkt.user\_id,

NAME\_SIZE);

pkt->pkttype = CDK\_PKT\_ATTRIBUTE;

if (rc)

return gnutls\_assert\_val(rc);

break;