CVE-2017-5336

描述：Stack-based buffer overflow in the cdk\_pk\_get\_keyid function in lib/opencdk/pubkey.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via a crafted OpenPGP certificate.

软件：GnuTLS 3.1.4

源码： lib/opencdk/pubkey.c

出现位置： 544-564行

关键源码：

{

u32 lowbits = 0;

byte buf[24];

int rc;

if (pk && (!pk->keyid[0] || !pk->keyid[1])) {

if (pk->version < 4 && is\_RSA(pk->pubkey\_algo)) {

size\_t n;

n = MAX\_MPI\_BYTES;

- \_gnutls\_mpi\_print(pk->mpi[0], p, &n);

+ rc = \_gnutls\_mpi\_print(pk->mpi[0], p, &n);

+ if (rc < 0 || n < 8) {

+ keyid[0] = keyid[1] = (u32)-1;

+ return (u32)-1;

+ }

+

pk->keyid[0] =

p[n - 8] << 24 | p[n - 7] << 16 | p[n -

6] << 8 |