CVE-2017-7860

描述：Google gRPC before 2017-02-22 has an out-of-bounds write caused by a heap-based buffer overflow related to the parse\_unix function in core/ext/client\_channel/parse\_address.c.

软件：Google gRPC

源码：src/core/ext/client\_channel/parse\_address.c

出现位置： 50-54行

关键源码：

int parse\_unix(grpc\_uri \*uri, grpc\_resolved\_address \*resolved\_addr) {

struct sockaddr\_un \*un = (struct sockaddr\_un \*)resolved\_addr->addr;

+ memset(un, 0, sizeof(\*un));

un->sun\_family = AF\_UNIX;

- strcpy(un->sun\_path, uri->path);

+ strncpy(un->sun\_path, uri->path, sizeof(un->sun\_path) - 1 /\* null term'd \*/);