CVE-2017-7246

描述：Stack-based buffer overflow in the pcre32\_copy\_substring function in pcre\_get.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (WRITE of size 268) or possibly have unspecified other impact via a crafted file.

软件：pcre-8.40

源码： pcre\_get.c

出现位置： 350-360行

关键源码：

{

int yield;

if (stringnumber < 0 || stringnumber >= stringcount)

return PCRE\_ERROR\_NOSUBSTRING;

stringnumber \*= 2;

yield = ovector[stringnumber+1] - ovector[stringnumber];

if (size < yield + 1) return PCRE\_ERROR\_NOMEMORY;

memcpy(buffer, subject + ovector[stringnumber], IN\_UCHARS(yield));

buffer[yield] = 0;

return yield;

}