CVE-2017-7245

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 4) or possibly have unspecified other impact via a crafted file.

软件：PCRE 8.40

源码： pcre\_get.c

出现位置： 358行

关键源码：

Pcre\_get.c:

pcre32\_copy\_substring(PCRE\_SPTR32 subject, int \*ovector, int stringcount,

int stringnumber, PCRE\_UCHAR32 \*buffer, int size)

#endif

{

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)); //溢出

buffer[yield] = 0;

return yield;

}

Pcretest.c 调用

for (i = 0; i < 32; i++)

{

if ((copystrings & (1 << i)) != 0)

{

int rc;

char copybuffer[256];

PCRE\_COPY\_SUBSTRING(rc, bptr, use\_offsets, count, i,

copybuffer, sizeof(copybuffer));

if (rc < 0)

fprintf(outfile, "copy substring %d failed %d\n", i, rc);

else

{

fprintf(outfile, "%2dC ", i);

PCHARSV(copybuffer, 0, rc, outfile);

fprintf(outfile, " (%d)\n", rc);

}

}

}