CVE-2017-6429

描述：Buffer overflow in the tcpcapinfo utility in Tcpreplay before 4.2.0 Beta 1 allows remote attackers to have unspecified impact via a pcap file with an over-size packet.

软件： Tcpreplay

源码： src/tcpcapinfo.c

出现位置： 258-282行

关键源码：

else {

/\* manually map on-disk bytes to our memory structure \*/

memcpy(&readword, buf, 4);

pcap\_ph.ts.tv\_sec = readword;

memcpy(&readword, &buf[4], 4);

pcap\_ph.ts.tv\_usec = readword;

memcpy(&pcap\_ph.caplen, &buf[8], 4);

memcpy(&pcap\_ph.len, &buf[12], 4);

if (swapped == 1) {

dbg(3, "Swapping packet header bytes...");

pcap\_ph.caplen = SWAPLONG(pcap\_ph.caplen);

pcap\_ph.len = SWAPLONG(pcap\_ph.len);

pcap\_ph.ts.tv\_sec = SWAPLONG(pcap\_ph.ts.tv\_sec);

pcap\_ph.ts.tv\_usec = SWAPLONG(pcap\_ph.ts.tv\_usec);

}

printf("%"PRIu64"\t%4"PRIu32"\t\t%4"PRIu32"\t\t%"

PRIx32".%"PRIx32,

pktcnt, pcap\_ph.len, pcap\_ph.caplen,

(unsigned int)pcap\_ph.ts.tv\_sec, (unsigned int)pcap\_ph.ts.tv\_usec);

if (pcap\_fh.snaplen < pcap\_ph.caplen) {

caplentoobig = 1;

}

caplen = pcap\_ph.caplen;

}