CVE-2017-7853

描述：In libosip2 in GNU oSIP 5.0.0, a malformed SIP message can lead to a heap buffer overflow in the msg\_osip\_body\_parse() function defined in osipparser2/osip\_message\_parse.c, resulting in a remote DoS.

软件： GNU oSIP 5.0.0

源码： src/osipparser2 / osip\_message\_parse.c

出现位置： 789-799行

关键源码：

/\* Skip CR before end boundary. \*/

if (\*(end\_of\_body - 1) == '\r')

body\_len--;

tmp = osip\_malloc (body\_len + 2);

if (tmp == NULL) {

osip\_free (sep\_boundary);

return OSIP\_NOMEM;

}

memcpy (tmp, start\_of\_body, body\_len);

tmp[body\_len] = '\0';