CVE-2016-10326

描述：In libosip2 in GNU oSIP 4.1.0, a malformed SIP message can lead to a heap buffer overflow in the osip\_body\_to\_str() function defined in osipparser2/osip\_body.c, resulting in a remote DoS.

软件：GNU oSIP 4.1.0 libosip2-4.1.0

源码：osipparser2 / osip\_body.c

出现位置： 419-421行

关键源码：

/\*In function osip\_body\_to\_str, the initially computed length for storing stringified SIP body length is incorrect because it does not anticipate the addition of the CRLF characters when body->body->content\_type is not NULL: \*/

// Incorrect computation

length = 15 + body->length + (osip\_list\_size (body->headers) \* 40);

tmp\_body = (char \*) osip\_malloc (length);

...

if ((osip\_list\_size (body->headers) > 0) || (body->content\_type != NULL)) {

// tmp\_body may overflow here

tmp\_body = osip\_strn\_append (tmp\_body, CRLF, 2);

}

memcpy (tmp\_body, body->body, body->length);

tmp\_body = tmp\_body + body->length;