CVE-2016-10325

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

软件：GNU oSIP 4.1.0 libosip2-4.1.0

源码：osipparser2 / osip\_message\_to\_str.c

出现位置： 346-384行

关键源码：

if (1 == osip\_message\_get\_\_property (sip)) { /\* message is already available in "message" \*/

\*dest = osip\_malloc (sip->message\_length + 1);

if (\*dest == NULL)

return OSIP\_NOMEM;

memcpy (\*dest, sip->message, sip->message\_length);

(\*dest)[sip->message\_length] = '\0';

if (message\_length != NULL)

\*message\_length = sip->message\_length;

return OSIP\_SUCCESS;

}

else {

/\* message should be rebuilt: delete the old one if exists. \*/

osip\_free (sip->message);

sip->message = NULL;

}

}

message = (char \*) osip\_malloc (SIP\_MESSAGE\_MAX\_LENGTH); /\* ???? message could be > 4000 \*/

if (message == NULL)

return OSIP\_NOMEM;

\*dest = message;

/\* add the first line of message \*/

i = \_\_osip\_message\_startline\_to\_str (sip, &tmp);

if (i != 0) {

if (!sipfrag) {

osip\_free (\*dest);

\*dest = NULL;

return i;

}

/\* A start-line isn't required for message/sipfrag parts. \*/

}

else {

message = osip\_str\_append (message, tmp);

osip\_free (tmp);

message = osip\_strn\_append (message, CRLF, 2);

}