CVE-2016-10324

描述：In libosip2 in GNU oSIP 4.1.0, a malformed SIP message can lead to a heap buffer overflow in the osip\_clrncpy() function defined in osipparser2/osip\_port.c.

软件：GNU oSIP 4.1.0 libosip2-4.1.0

源码：osipparser2 / osip\_port.c

出现位置： 1465-1487行

关键源码：

if (src == NULL)

return NULL;

/\* find the start of relevant text \*/

pbeg = src;

while ((' ' == \*pbeg) || ('\r' == \*pbeg) || ('\n' == \*pbeg) || ('\t' == \*pbeg))

pbeg++;

/\* find the end of relevant text \*/

pend = src + len - 1;

while ((' ' == \*pend) || ('\r' == \*pend) || ('\n' == \*pend) || ('\t' == \*pend)) {

pend--;

if (pend < pbeg) {

\*dst = '\0';

return dst;

}

}

/\* if pend == pbeg there is only one char to copy \*/

spaceless\_length = pend - pbeg + 1; /\* excluding any '\0' \*/

memmove (dst, pbeg, spaceless\_length);

p = dst + spaceless\_length;