CVE-2017-7875

描述：In wallpaper.c in feh before v2.18.3, if a malicious client pretends to be the E17 window manager, it is possible to trigger an out-of-boundary heap write while receiving an IPC message. An integer overflow leads to a buffer overflow and/or a double free.

软件：feh-2.18.2

源码：[src/wallpaper.c](https://github.com/derf/feh/commit/f7a547b7ef8fc8ebdeaa4c28515c9d72e592fb6d" \l "diff-6b3a68240b491abdfcfbd40e0bb3b23a" \o "src/wallpaper.c)

出现位置： 794-819 行

关键源码：

char \*enl\_ipc\_get(const char \*msg\_data)

{

static char \*message = NULL;

static unsigned short len = 0;

char buff[13], \*ret\_msg = NULL;

register unsigned char i;

unsigned char blen;

if (msg\_data == IPC\_TIMEOUT) {

return(IPC\_TIMEOUT);

}

for (i = 0; i < 12; i++) {

buff[i] = msg\_data[i];

}

buff[12] = 0;

blen = strlen(buff);

if (message != NULL) {

len += blen;

message = (char \*) erealloc(message, len + 1);

strcat(message, buff);

} else {

len = blen;

message = (char \*) emalloc(len + 1);

strcpy(message, buff);

}