

# Unlink

“

各个版本中unlink利用方法

## Glibc2.23

```
1  #define unlink(AV, P, BK, FD) {
2      if (__builtin_expect (chunksize(P) != prev_size (next_chunk(P)), 0))
3          \
4          malloc_printerr ("corrupted size vs. prev_size");
5          \
6          FD = P->fd;
7          \
8          BK = P->bk;
9          \
10         if (__builtin_expect (FD->bk != P || BK->fd != P, 0))
11             \
12             malloc_printerr ("corrupted double-linked list");
13             \
14         else {
15             \
16             FD->bk = BK;
17             \
18             BK->fd = FD;
19             \
20             if (!in_smallbin_range (chunksize_nomask (P))
21                 \
22                 && __builtin_expect (P->fd_nextsize != NULL, 0)) {
23                 \
24                 if (__builtin_expect (P->fd_nextsize->bk_nextsize != P, 0)
25                     \
26                     || __builtin_expect (P->bk_nextsize->fd_nextsize != P, 0))
27                     \
28                     malloc_printerr ("corrupted double-linked list (not small)");
29                     \
30                     if (FD->fd_nextsize == NULL) {
31                         \
32                         if (P->fd_nextsize == P)
33                             \
34                             FD->fd_nextsize = FD->bk_nextsize = FD;
35                             \
36                         else {
37                             \
38                             FD->fd_nextsize = P->fd_nextsize;
39                             \
40                             FD->bk_nextsize = P->bk_nextsize;
41                             \
42                             P->fd_nextsize->bk_nextsize = FD;
43                             \
44                             P->bk_nextsize->fd_nextsize = FD;
45                             \
46                         }
47                     }
48                 } else {
49                     \
50                     P->fd_nextsize->bk_nextsize = P->bk_nextsize;
51                     \
52                     P->bk_nextsize->fd_nextsize = P->fd_nextsize;
53                     \
54                 }
55             }
56         }
57     }
58 }
```

## Glibc2.27

唯一的差别就是在最开始加了对size的验证

```
1  if (chunksize(P) != prev_size (next_chunk(P)))  
2      malloc_printerr ("corrupted size vs. prev_size");
```