2025.11.14

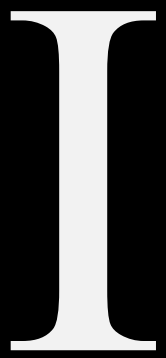
Fastbin / Unsortedbin

가디언 시스템 보안 & 취약점 분석 세미나 5.2

임준서

Fast, Unsorted bins

Glibc 2.35



Bins

Recap

Malloc

Tcachebin 〉(fastbin) 〉small/large bin 〉unsorted bin 〉miss

Free

Tcachebin 〉(fastbin) 〉unsorted bin

glibc 2.35에서는 calloc, realloc은 tcachebin을 사용하지 않는다!

임준서

Fastbin

Concept

Size (metadata 포함)

less than 0x90

Singly Linked List

No doubly linked list yet

One bin

e.g. 0x20 → 0x70 → 0x30 → 0x40 → ···

Fastbin

malloc

Base) tcache is used up

Case 1) size ∈ fastbin range

Case 2) size ∉ fastbin range

Fastbin

free

Base) tcache is filled up

Case 1) size ∈ fastbin range

Case 2) size ∉ fastbin range

Unsortedbin

Concept

큰 크기의 청크들이 들어감

Coalesce을 통해 효율 up

필요한 경우 chunk를 split

남은 청크는 small/large bin에 들어간다.

Security Mitigations

Glibc 2.35 – fastbin

II

Fastbin Mitigation

Double free

```
if (SINGLE_THREAD_P)
  {
    /* Check that the top of the bin is not the record we are going to
       add (i.e., double free).  */
    if (__builtin_expect (old == p, 0))
      malloc_printerr ("double free or corruption (fasttop)");
    p->fd = PROTECT_PTR (&p->fd, old);
    *fb = p;
  }
```

이전 청크만 확인한다!

_int_free

Fastbin Mitigation

Corrupted Chunk

```
if (__glibc_likely (victim != NULL))
  {
    size_t victim_idx = fastbin_index (chunksize (victim));
    if (__builtin_expect (victim_idx != idx, 0))
      malloc_printerr ("malloc(): memory corruption (fast)");
    check_remalloced_chunk (av, victim, nb);
```

할당되는 청크의 크기 = 이전 청크 크기

_int_malloc

Unsorted Mitigation

Corrupted Chunk

```
if (__glibc_unlikely (size <= CHUNK_HDR_SZ)
    || __glibc_unlikely (size > av->system_mem))
  malloc_printerr ("malloc(): invalid size (unsorted)");
if (__glibc_unlikely (chunksize_nomask (next) < CHUNK_HDR_SZ)
    || __glibc_unlikely (chunksize_nomask (next) > av->system_mem))
  malloc_printerr ("malloc(): invalid next size (unsorted)");
if (__glibc_unlikely ((prev_size (next) & ~(SIZE_BITS)) != size))
  malloc_printerr ("malloc(): mismatching next->prev_size (unsorted)");
if (__glibc_unlikely (bck->fd != victim)
    || __glibc_unlikely (victim->fd != unsorted_chunks (av)))
  malloc_printerr ("malloc(): unsorted double linked list corrupted");
if (__glibc_unlikely (prev_inuse (next)))
  malloc_printerr ("malloc(): invalid next->prev_inuse (unsorted)");
```

이것들 전부 통과 필요, 이후에도 더 있음

_int_malloc

Fastbin Dup

Glibc 2.35

III

Fastbin Dup

Concept

UaF 같은 게 있으면 사실 tcache가 더 편함

주로 Double free만 있을 때 사용

A → B → A → B → …

free(A); free(B); free(A);

Example

Fastbin reverse into tcache

AAR/AAW 1회 가능, UaF

1. Tcache(7) fill
2. Setup size chunk at (target-0x8)
3. Make 6 fastbin entries and modify the last one to point to (target)
4. Flush tcache(7)
5. Malloc will load fastbin entries in reverse order, our target being the first.

https://github.com/shellphish/how2heap/blob/master/glibc_2.35/fastbin_reverse_into_tcache.c

Example

Fastbin dup into tcache

AAR/AAW 1회 가능, Double Free

1. Tcache(7) fill
2. Fastbin dup
   7 → 8 → 7 ← …
3. Tache(7) flush
4. Next time we malloc, we get 7 as allocated and
   tcache[3] → 8 → 7 → 8 ← … as tcache
5. Chage the next* as we have 7^{th} chunk!

Example

house of botcake

AAR/AAW 1회 가능

1. Tcache(7) fill
2. Two unsortedbin(7, 8) which will coalesce
3. Free one tcache
4. Double free chunk 8
   Now, chunk 8 is in unsorted and tcache
5. Change next* of 8 by allocating chunks
   that will use up unsorted bin

github.com/shellphish/how2heap/blob/master/glibc_2.35/house_of_botcake.c

2025.11.14

Q&A

질문이 있다면 하십시오

임준서

2.5cm-2.5cm 떨어진 제목 36px

제목 하단의 부제목 18px

3.5cm 떨어진 내용 1 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

3.5cm 떨어진 내용 2 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

3.5cm 떨어진 내용 3 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

1cm-1cm 떨어진 주석 12px

1cm-1cm 떨어진 주석 12px

임준서

2.5cm-3.5cm 떨어진 제목 36px

제목 하단의 부제목 18px

3.5cm 떨어진 내용 1 32px

```
Git init
Git status
Git add text.txt
Git add .
Git commit
Ctrl+C
Git commit -m “genesis”
Git log
Git log --oneline
```

```
Git add .
Git reset .
Git commit -m “add README”
Git log --oneline -n 3
Git commit –a –m “hello”
```

1cm-1cm 떨어진 주석 12px

1cm-1cm 떨어진 주석 12px

중심에서 0.3cm 떨어진 소속 18px