


New issue

Jump to bottom

## double free in update\_read\_cache\_bitmap\_v3\_order #6013

 Closed hac425xxx opened this issue on Mar 31, 2020 · 2 comments

Labels **fixed-waiting-test**

Milestone  2.0.0

hac425xxx commented on Mar 31, 2020

version

<https://github.com/FreeRDP/FreeRDP/blob/9ef1e81c559bb19d613b4da2d68908ea5d7f9259/libfreerdp/core/orders.c#L2167>

vuln code

update\_read\_cache\_bitmap\_v3\_order first read new\_len from stream, and pass the new\_len to realloc

Then it could call realloc(bitmapData->data, 0), this could free bitmapData->data, and return NULL

realloc function source code

```
void *__libc_realloc(void *oldmem, size_t bytes)
{
    if (bytes == 0 && oldmem != NULL) // if bytes =0, it could free(oldmem).
    {
        __libc_free(oldmem);
        return 0;
    }
}
```

when new\_data is NULL, it could call free\_cache\_bitmap\_v3\_order to free bitmapData->data again.

Double Free!

function code.

```
static CACHE_BITMAP_V3_ORDER* update_read_cache_bitmap_v3_order
{
    Stream_Read_UINT32(s, new_len); // if new_len = 0

    if (Stream_GetRemainingLength(s) < new_len) //pass this check
        goto fail;

    new_data = (BYTE*)realloc(bitmapData->data, new_len); // realloc could free bitmapData->data

    if (!new_data) // new_data could be NULL
        goto fail;

fail:
    free_cache_bitmap_v3_order(update->context, cache_bitmap_v3); // free bitmapData->data again.
    return NULL;
}
```

hac425xxx commented on Mar 31, 2020

Author

code to test realloc action

```
#include<stdlib.h>



int main()
{
    char* p = malloc(0x30);



    char* x = realloc(p, 0);

    printf("x:%x\n", x);

    free(p);

    return 0;
}
```

  akallabeth added this to the 2.0.0 milestone on Mar 31, 2020

  akallabeth added the fixed-waiting-test label on Apr 2, 2020

 nfedera closed this as completed in 67c2aa5 on Apr 6, 2020

---

  **bmiklautz** mentioned this issue on May 6, 2020

could you please request some cve for issue 6005~6013 #6027

 Closed

**carnil** commented on May 8, 2020

CVE-2020-11044 was assigned for this issue.

Assignees

No one assigned

Labels

**fixed-waiting-test**

Projects

None yet

Milestone

2.0.0

Development

No branches or pull requests

3 participants

