

New issue

Jump to bottom

# memory out of bounds read in rdp\_read\_share\_control\_header #6008

 Closed hac425xxx opened this issue on Mar 31, 2020 · 0 comments · Fixed by #6019

Labels fixed-waiting-test  
Milestone 2.0.0

hac425xxx commented on Mar 31, 2020 · edited

```
version
https://github.com/FreeRDP/FreeRDP/blob/9ef1e81c559bb19d613b4da2d6898ea5d7f9259/11bfreerdp/core/rdp.c#L1129

vuln code
if Stream_GetRemainingLength(s) = 5 and *length = 5 , it could one byte overflow read in Stream_Read_UINT16(s, *channel_id);





BOOL rdp_read_share_control_header(wStream* s, UINT16* length, UINT16* type, UINT16* channel_id)
{
    if (Stream_GetRemainingLength(s) < 2)
        return FALSE;

    Stream_Read_UINT16(s, *length); /* totalLength */



    if (((size_t)*length - 2) > Stream_GetRemainingLength(s))
        return FALSE;

    Stream_Read_UINT16(s, *type); /* pduType */
    *type &= 0x0F; /* type is in the 4 least significant bits */

    if (*length > 4)
        Stream_Read_UINT16(s, *channel_id); // memory out of bounds read
    return TRUE;
}
```

-  akallabeth added this to the 2.0.0 milestone on Mar 31, 2020
-  akallabeth added fixed-waiting-test and removed fixed-waiting-test labels on Apr 2, 2020
-  akallabeth linked a pull request on Apr 6, 2020 that will close this issue
- Fix issues with boundary access. #6019
-  akallabeth closed this as completed on Apr 6, 2020

Merged


 bmiklantz mentioned this issue on May 6, 2020  
could you please request some cve for issue 6005~6013 #6027  


Assignees  
No one assigned

Labels  
fixed-waiting-test

Projects  
None yet

Milestone  
2.0.0

Development  
Successfully merging a pull request may close this issue.  
 Fix issues with boundary access.  
akallabeth/FreeRDP

2 participants  
