New issue

Jump to bottom

memory out of bounds read in rdp_read_flow_control_pdu #6007

Closed hac425xxx opened this issue on Mar 31, 2020 · 0 comments

Labels fixed-waiting-test

Milestone 2.0.0

hac425xxx commented on Mar 31, 2020 • edited

version

```
https://github.com/FreeRDP/FreeRDP/blob/9ef1e81c559bb19d613b4da2d68908ea5d7f9259/libfreerdp/core/rdp.c#L1129
```

vuln code

`rdp_read_share_control_header` could read 2 byte from stream, if `*length == 0x8000` , it could call `rdp_read_flow_control_pdu` .

```
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 (*length == 0x8000)
        {
                rdp_read_flow_control_pdu(s, type);   // vuln function
```

`rdp_read_flow_control_pdu` just read 1byte and seek some byte from stream without check length, it could `lead _s->pointer - _s->buffer > _s->length` , then the check in other function could failed

```
void rdp_read_flow_control_pdu(wStream* s, UINT16* type)
{

        UINT8 pduType;
        Stream_Read_UINT8(s, pduType); /* pduTypeFlow */
        *type = pduType;
        Stream_Seek_UINT8(s);  /* pad8bits */
        Stream_Seek_UINT8(s);  /* flowIdentifier */
        Stream_Seek_UINT8(s);  /* flowNumber */
        Stream_Seek_UINT16(s); /* pduSource */
}
```

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 `9301bfe` on Apr 6, 2020

bmiklautz mentioned this issue on May 6, 2020

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

Closed

Assignees

No one assigned

Labels

fixed-waiting-test

Projects

None yet

Milestone

2.0.0

Development

No branches or pull requests

2 participants