New issue

Jump to bottom

memory out of bounds read in update_read_icon_info #6010

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/window.c#L187
```

vuln code

`update_read_icon_info` first read `iconInfo->cbColorTable` , `iconInfo->cbBitsMask` and `iconInfo->cbBitsColor` from the wStream,

```
static BOOL update_read_icon_info(wStream* s, ICON_INFO* iconInfo)
{
        ...............................................
        ...............................................
                        Stream_Read_UINT16(s, iconInfo->cbColorTable); /* cbColorTable (2 bytes) */
                        break;
        }
        //
        Stream_Read_UINT16(s, iconInfo->cbBitsMask);  /* cbBitsMask (2 bytes) */
        Stream_Read_UINT16(s, iconInfo->cbBitsColor); /* cbBitsColor (2 bytes) */
```

And then it check cbBitsMask and cbBitsColor

```
        if (Stream_GetRemainingLength(s) < iconInfo->cbBitsMask + iconInfo->cbBitsColor)
                return FALSE;
```

Then it could call Stream_Read to read data from s, size is `cbBitsMask+cbColorTable+cbBitsColor`

```
        ............................................................................................
        ............................................................................................
        ............................................................................................
        Stream_Read(s, iconInfo->bitsMask, iconInfo->cbBitsMask);

        ............................................................................................
        ............................................................................................

                Stream_Read(s, iconInfo->colorTable, iconInfo->cbColorTable);

        ............................................................................................
        ............................................................................................
        Stream_Read(s, iconInfo->bitsColor, iconInfo->cbBitsColor);
```

so when `cbBitsMask+cbBitsColor < Stream_GetRemainingLength(s)` and `cbBitsMask+cbColorTable+cbBitsColor > Stream_GetRemainingLength(s)` , it could lead memory out of bounds read

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

akallabeth added a commit to akallabeth/FreeRDP that referenced this issue on Apr 2, 2020

`Fix FreeRDP#6010: Check length in read_icon_info` 1237662

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

nfedera closed this as completed in `6b2bc41` 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-2020-11042 was assigned for this issue.

tcullum-rh commented on May 14, 2020

@akallabeth @hac425xxx Does this function accept untrusted input (icon metadata packet) from anywhere or only from an established RDP connection? Trying to assess impact. Thanks.

Assignees

No one assigned

Labels

fixed-waiting-test

Projects

None yet

Milestone

2.0.0

Development

No branches or pull requests

4 participants