New issue

Jump to bottom

memory out of bounds read in update_read_bitmap_data #6005

Closed hac425xxx opened this issue on Mar 30, 2020 · 4 comments

Labels fixed-waiting-test

Milestone 2.0.0

hac425xxx commented on Mar 30, 2020

vuln code

```
static BOOL update_read_bitmap_data(rdpUpdate* update, wStream* s, BITMAP_DATA* bitmapData)
{
	WINPR_UNUSED(update);
	if (Stream_GetRemainingLength(s) < 18)
		return FALSE;

	Stream_Read_UINT16(s, bitmapData->destLeft);
	Stream_Read_UINT16(s, bitmapData->destTop);
	Stream_Read_UINT16(s, bitmapData->destRight);
	Stream_Read_UINT16(s, bitmapData->destBottom);
	Stream_Read_UINT16(s, bitmapData->width);
	Stream_Read_UINT16(s, bitmapData->height);
	Stream_Read_UINT16(s, bitmapData->bitsPerPixel);
	Stream_Read_UINT16(s, bitmapData->flags);
	Stream_Read_UINT16(s, bitmapData->bitmapLength);

       // now use 18 byte in s


	if (bitmapData->flags & BITMAP_COMPRESSION)
	{
		if (!(bitmapData->flags & NO_BITMAP_COMPRESSION_HDR))
		{
			// below read data from stream without check stream's size
			Stream_Read_UINT16(s,
					bitmapData->cbCompFirstRowSize); /* cbCompFirstRowSize (2 bytes) */
			Stream_Read_UINT16(s,
					bitmapData->cbCompMainBodySize); /* cbCompMainBodySize (2 bytes) */
			Stream_Read_UINT16(s, bitmapData->cbScanWidth);     /* cbScanWidth (2 bytes) */
			Stream_Read_UINT16(s,
					bitmapData->cbUncompressedSize); /* cbUncompressedSize (2 bytes) */
			bitmapData->bitmapLength = bitmapData->cbCompMainBodySize;
		}

		bitmapData->compressed = TRUE;
	}
	else
		bitmapData->compressed = FALSE;

	if (Stream_GetRemainingLength(s) < bitmapData->bitmapLength)
		return FALSE;
```

The function first verifies that the length of s cannot be less than 18, and then reads 18 bytes later.

If `bitmapData-> flags & BITMAP_COMPRESSION` and `! (BitmapData-> flags & NO_BITMAP_COMPRESSION_HDR)` , it will continue to read data from the stream without check if the length in the stream is enough

hac425xxx commented on Mar 30, 2020 Author

suggestion:

check stream's length before read it

hac425xxx commented on Mar 30, 2020 Author

branch

```
https://github.com/FreeRDP/FreeRDP/blob/9ef1e81c559bb19d613b4da2d68908ea5d7f9259/libfreerdp/core/update.c#L106
```

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

bmiklautz commented on Mar 31, 2020 Member

@hac425xxx Thank you. Just as note it would be nice if you contact us before opening a security related issue.

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

nfedera closed this as completed in `f8890a6` 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-2020-11045 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

4 participants