POC2 analysis:

Vulnerability type: integer overflow

Function gdi_RectToCRgn can cause integer overflow when reading the width of a bitmap

```
/**
 * Convert a rectangle to region coordinates.
 * @param rect source rectangle
 * @param x x1
 * @param y y1
 * @param w width
 * @param h height
 */

INLINE void gdi_RectToCRgn(const HGDI_RECT rect,
                           INT32* x, INT32* y,
                           INT32* w, INT32* h)
{
    *x = rect->left;
    *y = rect->top;
    *w = rect->right - rect->left + 1;
    *h = rect->bottom - rect->top + 1;  已用时间 <= 1ms
}
```

Next, when the bitmap data is cached, nWidth * formatsize will cause a copy of a large value range, causing a heap overflow.

```
            srcp = gdi_get_bitmap_pointer(hdc, nXDest, nYDest);
            formatSize = GetBytesPerPixel(hdc->format);

            for (y = 1; y < nHeight; y++)
            {
                BYTE* dstp = gdi_get_bitmap_pointer(hdc, nXDest, nYDest + y);
                memcpy(dstp, srcp, nWidth * formatSize);
            }

            break;
```