memory out of bounds read in autodetect_recv_bandwidth_measure_results #6009

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

version

```
https://github.com/FreeRDP/FreeRDP/blob/9ef1e81c559bb19d613b4da2d68908ea5d7f9259/libfreerdp/core/autodetect.c#L459
```

vuln code

autodetect_recv_bandwidth_measure_results read 8 bytes from stream without check stream's length

```
static BOOL autodetect_recv_bandwidth_measure_results(rdpRdp* rdp, wStream* s,
                                                      AUTODETECT_RSP_PDU* autodetectRspPdu)
{
        BOOL success = TRUE;

        if (autodetectRspPdu->headerLength != 0x0E)
                return FALSE;

        WLog_VRB(AUTODETECT_TAG, "received Bandwidth Measure Results PDU");
        Stream_Read_UINT32(s, rdp->autodetect->bandwidthMeasureTimeDelta); /* timeDelta (4 bytes) */
        Stream_Read_UINT32(s, rdp->autodetect->bandwidthMeasureByteCount); /* byteCount (4 bytes) */
```

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 `f5e73cc` 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