Suricata - Bug #3349

Suricata 5.0 crashes while rule reload

11/20/2019 04:16 AM - haiwei liu

Status: Closed
Priority: Normal
Assignee: OISF Dev
Category: TBD
Target version: TBD
Affected Versions: 5.0.0
Effort:

Description
Suricata 5.0 crashes while rule reload and performing flow detect.

Backtrace
#0 0x00007f6ce86e337 in raise () from /lib64/libc.so.6
#1 0x00007f6ce86fa28 in abort () from /lib64/libc.so.6
#2 0x00007f6ce80e087 in __libc_message () from /lib64/libc.so.6
#3 0x00007f6ce8b9679 in _int_free () from /lib64/libc.so.6
#4 0x000000000004a43f in DetectEngineThreadCtxFree (det_ctx=0x7fb6a4a96ce0) at detect-engine.c:25
#5 0x000000000004ad8f7 in DetectEngineThreadCtxDeinit (tv=<optimized out>, data=0x7fb6a4a96ce0) at detect-engine.c:2604
#6 0x000000000004ae090 in DetectEngineReloadThreads (new_de_ctx=new_de_ctx@entry=0xa8dcf20) at detect-engine.c:1543
#7 0x000000000004b1890 in DetectEngineReload (suri=suri@entry=0xa81100 <suricata>) at detect-engine.c:3680
#8 0x0000000000041fd55 in SuricataMainLoop (suri=<optimized out>) at suricata.c:2860
#9 main (argc=<optimized out>, argv=<optimized out>) at suricata.c:3021

reason:

InspectionBuffer *InspectionBufferGet(DetectEngineThreadCtx *det_ctx, const int list_id)
{
    InspectionBuffer *buffer = &det_ctx->inspect.buffers[list_id];
    if (buffer->inspect == NULL) {
        det_ctx->inspect.to_clear_queue[det_ctx->inspect.to_clear_idx++] = list_id;
    }
    return buffer;
}

The size of det_ctx->inspect.to_clear_idx will exceed det_ctx->inspect.buffers_size during run, resulting in memory out of bounds.

History
#1 - 11/20/2019 07:12 AM - Victor Julien
- Description updated
- Assignee changed from Victor Julien to OISF Dev
- Priority changed from High to Normal
- Target version changed from 5.0.0 to 5.0.1
- Affected Versions 5.0.0 added
- Affected Versions deleted (5.0beta1)

#2 - 11/20/2019 07:33 AM - Victor Julien
What rules are you using?

03/09/2022
Hi, we're closing this issue since there have been no further responses. If you think this issue is still relevant, try to test it again with the most recent version of suricata and reopen the issue. If you want to improve the bug report please take a look at https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Reporting_Bugs

This was fixed in 5.0.7. See ticket #4485.