Suricata - Bug #2458
memleak: gitmaster - 4.1.0-dev (rev c60decd)
03/19/2018 06:07 PM - Peter Manev

Status: Assigned
Priority: Normal
Assignee: Jeff Lucovsky
Category: TBD
Affected Versions:
Difficulty:
Effort:
Label:

Description

Seeing some ftp related memleaks it seams with gitmaster - 4.1.0-dev (rev c60decd) on live traffic.

---1217---ERROR: LeakSanitizer: detected memory leaks

Direct leak of 64 byte(s) in 2 object(s) allocated from:
#0 0x4bffe0 in calloc (/usr/local/bin/suricata+0x4bffe0)
#1 0x629872 in FTPCalloc /home/pevman/tests/git/suricata/src/app-layer-ftp.c:154:11
#2 0x62776b in FTPParseRequest /home/pevman/tests/git/suricata/src/app-layer-ftp.c:441:51
#3 0x6638a3 in AppLayerParserParse /home/pevman/tests/git/suricata/src/app-layer-parser.c:1142:13
#4 0x527985 in AppLayerHandleTCPData /home/pevman/tests/git/suricata/src/app-layer.c:635:17
#5 0xc8a52b in ReassembleUpdateAppLayer /home/pevman/tests/git/suricata/src/stream-tcp-reassemble.c:1063:13
#6 0xc89397 in StreamTcpReassembleAppLayer /home/pevman/tests/git/suricata/src/stream-tcp-reassemble.c:1136:12
#7 0x88c883 in StreamTcpReassembleHandleSegmentUpdateACK /home/pevman/tests/git/suricata/src/stream-tcp-reassemble.c:1685:9
#8 0xc8f94a in StreamTcpReassembleHandleSegment /home/pevman/tests/git/suricata/src/stream-tcp-reassemble.c:1724:9
#9 0xc77200 in HandleEstablishedPacketToClient /home/pevman/tests/git/suricata/src/stream-tcp.c:2360:9
#10 0xc2af1a in StreamTcpPacketStateEstablished /home/pevman/tests/git/suricata/src/stream-tcp.c:2597:13
#11 0x1c112d22 in StreamTcpPacket /home/pevman/tests/git/suricata/src/stream-tcp.c:4643:20
#12 0x5300ec in StreamTcp /home/pevman/tests/git/suricata/src/stream-tcp.c:5018:11
#13 0x215c4d in FlowWorker /home/pevman/tests/git/suricata/src/flow-worker.c:216:9
#14 0xc422d0 in TmThreadsSlotVarRun /home/pevman/tests/git/suricata/src/tm-threads.c:145:17
#15 0x26075bb in TmThreadsSlotProcessPkt /home/pevman/tests/git/suricata/src/tm-threads.c:147:9
#16 0x8be0e6d in AFParsePacketV3 /home/pevman/tests/git/suricata/src/source-af-packet.c:1116:9
#17 0x8b7a70 in AFParkBlock /home/pevman/tests/git/suricata/src/source-af-packet.c:1131:13
#18 0x2bbcc37 in AFPreadFromRingV3 /home/pevman/tests/git/suricata/src/source-af-packet.c:1170:13
#19 0x8bb969e in ReceiveAFLoop /home/pevman/tests/git/suricata/src/source-af-packet.c:1559:17
#20 0xcd6cfe in TmThreadsSlotPktAcqLoop /home/pevman/tests/git/suricata/src/tm-threads.c:348:1
#21 0x7fdce678d6b9 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76b9)

Indirect leak of 80 byte(s) in 2 object(s) allocated from:
#0 0x4bffe0 in calloc (/usr/local/bin/suricata+0x4bffe0)
#1 0x629872 in FTPCalloc /home/pevman/tests/git/suricata/src/app-layer-ftp.c:154:11
#2 0x62776b in FTPParseRequest /home/pevman/tests/git/suricata/src/app-layer-ftp.c:446:39
#3 0x6638a3 in AppLayerParserParse /home/pevman/tests/git/suricata/src/app-layer-parser.c:1142:13
#4 0x527985 in AppLayerHandleTCPData /home/pevman/tests/git/suricata/src/app-layer.c:635:17
#5 0xc8a52b in ReassembleUpdateAppLayer /home/pevman/tests/git/suricata/src/stream-tcp-reassemble.c:1063:13
#6 0xc89397 in StreamTcpReassembleAppLayer /home/pevman/tests/git/suricata/src/stream-tcp-reassemble.c:1136:12
#7 0xc8fc83 in StreamTcpReassembleHandleSegmentUpdateACK /home/pevman/tests/git/suricata/src/stream-tcp-reassemble.c:1685:9
#8 0xc8f94a in StreamTcpReassembleHandleSegment /home/pevman/tests/git/suricata/src/stream-tcp-reassemble.c:1724:9
#9 0xc77200 in HandleEstablishedPacketToClient /home/pevman/tests/git/suricata/src/stream-tcp.c:2360:9
#10 0xc2afla in StreamTcpPacketStateEstablished /home/pevman/tests/git/suricata/src/stream-tcp.c:2597:13
#11 0xc11d22 in StreamTcpPacket /home/pevman/tests/git/suricata/src/stream-tcp.c:4643:20
#12 0xc530ec in FlowWorker /home/pevman/tests/git/suricata/src/stream-tcp.c:216:9
#13 0xbcc7a0 in AFPReadFromRingV3 /home/pevman/tests/git/suricata/src/source-af-packet.c:1131:13
#14 0xbbcc37 in AFPParsePacketV3 /home/pevman/tests/git/suricata/src/source-af-packet.c:1116:9
#15 0xbb969e in ReceiveAFPLoop /home/pevman/tests/git/suricata/src/source-af-packet.c:1559:17
#16 0xbb6de3 in TmThreadsSlotVarRun /home/pevman/tests/git/suricata/src/tm-threads.c:147:13
#17 0xbb6d9e in TmThreadsSlotProcessPkt /home/pevman/tests/git/suricata/src/tm-threads.c:348:13
#18 0x7fdce678d6b9 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76b9)

Related issues:
- Related to Bug #3118: asan leaks with 5.0.0-dev (9e126b210 2019-08-07) Closed
- Related to Bug #3378: ftp: asan detects leaks of expectations Closed

build-info attached.

History
#1 - 03/20/2018 05:45 AM - Victor Julien
- Assignee set to OISF Dev
- Target version set to TBD

No pcap I assume?

#2 - 03/20/2018 06:02 AM - Peter Manev
Unfortunately not. It happens on one of the live traffic test boxes and not all the time (every day).

#3 - 03/20/2018 07:31 AM - Eric Leblond
I've tried to play my FTP pcap sample by just looking at port 21 but no leak were seen. I was expecting a potential problem with the cleaning of expectation but it does not seem to be the case.

#4 - 03/24/2018 02:44 PM - Alexander Gozman
Eric Leblond wrote:

> I've tried to play my FTP pcap sample by just looking at port 21 but no leak were seen. I was expecting a potential problem with the cleaning of expectation but it does not seem to be the case.

Could it be that AppLayerExpectationHandle() leaks memory? For instance (app-layer-expectation.c:310):

```c
exp->data = NULL;
exp = RemoveExpectationAndGetNext(ipp, pexp, exp, lexp);
continue;
```

The place looks strange to me, especially when exp->data is not NULLed below when cleaning up old entries. However I don't know all the details and may be wrong.

#5 - 05/07/2019 03:04 PM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Jeff Lucovsky

Looks similar to https://github.com/OISF/suricata/pull/3827#discussion_r281012429

05/27/2020
Victor Julien wrote:

Looks similar to https://github.com/OISF/suricata/pull/3827#discussion_r281012429

That was a different issue, caused by changes in the PR itself.

#7 - 09/22/2019 12:47 PM - Jeff Lucovsky
- Related to Bug #3118: asan leaks with 5.0.0-dev (9e126b210 2019-08-07) added

#8 - 12/07/2019 03:12 PM - Jeff Lucovsky
- Related to Bug #3378: ftp: asan detects leaks of expectations added

#9 - 05/26/2020 10:23 AM - Victor Julien
Is this still relevant? Anyone still observing it?

#10 - 05/26/2020 11:00 AM - Peter Manev
not me, not anymore.

Files

build-info 3.58 KB 03/19/2018 Peter Manev