Suricata - Bug #3378
ftp: asan detects leaks of expectations
12/04/2019 08:29 AM - Peter Manev

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Eric Leblond</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>6.0.0rc1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td>Needs backport to 4.1, Needs backport to 5.0</td>
</tr>
</tbody>
</table>

**Description**

I can consistently reproduce the below upon exit/stopping Suricata on live traffic. (it seems related to - [https://redmine.openinfosecfoundation.org/issues/3118](https://redmine.openinfosecfoundation.org/issues/3118))

```plaintext
[39354] 4/12/2019 -- 08:32:53 - (util-mpm-hs.c:1081) <Perf> (MpmHSGlobalCleanup) -- Cleaning up Hyperscan global scratch
[9/1846]

=================================================================
==39354==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 32 byte(s) in 1 object(s) allocated from:
  #0 0x4cf5ea in calloc (/usr/bin/suricata+0x4cf5ea)
  #1 0x640184 in FTPCalloc /opt/suricata/src/app-layer-ftp.c:221:11
  #2 0x63a89c in FTPParseRequest /opt/suricata/src/app-layer-ftp.c:633:51
  #3 0x683be4 in AppLayerParserParse /opt/suricata/src/app-layer-parser.c:1239:13
  #4 0x535ca0 in AppLayerHandleTCPData /opt/suricata/src/app-layer.c:660:17
  #5 0xda4357 in ReassembleUpdateAppLayer /opt/suricata/src/stream-tcp-reassemble.c:1065:11
  #6 0xda2eb8 in StreamTcpReassembleAppLayer /opt/suricata/src/stream-tcp-reassemble.c:1122:12
  #7 0xda4d07 in StreamTcpReassembleHandleSegmentUpdateACK /opt/suricata/src/stream-tcp-reassemble.c:1696:9
  #8 0xda9d60 in StreamTcpReassembleHandleSegment /opt/suricata/src/stream-tcp-reassemble.c:1739:9
     ... 9
  #22 0x7f72f5719fa2 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x7fa2)

Indirect leak of 61 byte(s) in 1 object(s) allocated from:
  #0 0x4cf5ea in calloc (/usr/bin/suricata+0x4cf5ea)
  #1 0x640184 in FTPCalloc /opt/suricata/src/app-layer-ftp.c:221:11
  #2 0x63a89c in FTPParseRequest /opt/suricata/src/app-layer-ftp.c:633:39
  #3 0x683be4 in AppLayerParserParse /opt/suricata/src/app-layer-parser.c:1239:13
  #4 0x535ca0 in AppLayerHandleTCPData /opt/suricata/src/app-layer.c:660:17
  #5 0xda4357 in ReassembleUpdateAppLayer /opt/suricata/src/stream-tcp-reassemble.c:1065:11
  #6 0xda2eb8 in StreamTcpReassembleAppLayer /opt/suricata/src/stream-tcp-reassemble.c:1122:12
  #7 0xda4d07 in StreamTcpReassembleHandleSegmentUpdateACK /opt/suricata/src/stream-tcp-reassemble.c:1696:9
  #8 0xda9d60 in StreamTcpReassembleHandleSegment /opt/suricata/src/stream-tcp-reassemble.c:1739:9
     ... 9
  #22 0x7f72f5719fa2 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x7fa2)
```

05/27/2020
SUMMARY: AddressSanitizer: 93 byte(s) leaked in 2 allocation(s).

Suri info

This is Suricata version 5.0.1-dev (4343d1bc0 2019-11-30)
Features: PCAP_SET_BUFF AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HAVE_HTP_URI_NORMALIZE_HO
OK PCRE_JIT HAVE_NSS HAVE_LUA HAVE_LUAJIT HAVE_LIBJANSSON TLS MAGIC RUST
SIMD support: SSE_4_2 SSE_4_1 SSE_3
Atomic intrinsics: 1 2 4 8 16 byte(s)
64-bits, Little-endian architecture
GCC version 4.2.1 Compatible Clang 7.0.1 (tags/RELEASE_701-final), C version 199901
compiled with _FORTIFY_SOURCE=0
L1 cache line size (CLS)=64
thread local storage method: __thread
compiled with LibHTP v0.5.31, linked against LibHTP v0.5.31

Suricata Configuration:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF_PACKET support:</td>
<td>yes</td>
</tr>
<tr>
<td>eBPF support:</td>
<td>yes</td>
</tr>
<tr>
<td>XDP support:</td>
<td>yes</td>
</tr>
<tr>
<td>PF_RING support:</td>
<td>no</td>
</tr>
<tr>
<td>NFQueue support:</td>
<td>no</td>
</tr>
<tr>
<td>NFLOG support:</td>
<td>no</td>
</tr>
<tr>
<td>IPFW support:</td>
<td>no</td>
</tr>
<tr>
<td>Netmap support:</td>
<td>no</td>
</tr>
<tr>
<td>DAG enabled:</td>
<td>no</td>
</tr>
<tr>
<td>Napatech enabled:</td>
<td>no</td>
</tr>
<tr>
<td>WinDivert enabled:</td>
<td>no</td>
</tr>
<tr>
<td>Unix socket enabled:</td>
<td>yes</td>
</tr>
<tr>
<td>Detection enabled:</td>
<td>yes</td>
</tr>
<tr>
<td>Libmagic support:</td>
<td>yes</td>
</tr>
<tr>
<td>libnss support:</td>
<td>yes</td>
</tr>
<tr>
<td>libnsspr support:</td>
<td>yes</td>
</tr>
<tr>
<td>libjansson support:</td>
<td>yes</td>
</tr>
<tr>
<td>hiredis support:</td>
<td>no</td>
</tr>
<tr>
<td>hiredis async with libevent:</td>
<td>no</td>
</tr>
<tr>
<td>Prelude support:</td>
<td>no</td>
</tr>
<tr>
<td>PCRE jit:</td>
<td>yes</td>
</tr>
<tr>
<td>LUA support:</td>
<td>yes, through luajit</td>
</tr>
<tr>
<td>libluajit:</td>
<td>yes</td>
</tr>
<tr>
<td>GeoIP2 support:</td>
<td>yes</td>
</tr>
<tr>
<td>Non-bundled http:</td>
<td>no</td>
</tr>
<tr>
<td>Old barnyard2 support:</td>
<td>no</td>
</tr>
<tr>
<td>Hyperscan support:</td>
<td>yes</td>
</tr>
<tr>
<td>Libnet support:</td>
<td>yes</td>
</tr>
</tbody>
</table>
liblz4 support: yes
Rust support: yes
Rust strict mode: yes
Rust compiler path: /root/.cargo/bin/rustc
Rust compiler version: rustc 1.39.0 (4560ea788 2019-11-04)
Cargo path: /root/.cargo/bin/cargo
Cargo version: cargo 1.39.0 (1c6ec66d5 2019-09-30)
Python support: yes
Python path: /usr/bin/python3
Python distutils yes
Python yaml no
Install suricatactl: yes
Install suricatasc: yes
Install suricata-update: not bundled
Profiling enabled: no
Profiling locks enabled: no
Development settings:
Coccinelle / spatch: no
Unit tests enabled: no
Debug output enabled: no
Debug validation enabled: no
Generic build parameters:
Installation prefix: /usr
Configuration directory: /etc/suricata/
Log directory: /var/log/suricata/
--prefix /usr
--sysconfdir /etc
--localstatedir /var
--datarootdir /usr/share
Host: x86_64-pc-linux-gnu
Compiler: clang (exec name) / clang (real)
GCC Protect enabled: no
GCC march native enabled: yes
GCC Profile enabled: no
Position Independent Executable enabled: no
PCAP_CFLAGS -I/usr/include
SECCFLAGS

Related issues:
Related to Bug #2458: memleak: gitmaster - 4.1.0-dev (rev c60decd) Assigned
Has duplicate Bug #3455: asan ftp related leaks on the current gitmaster Closed
Copied to Bug #3596: ftp: asan detects leaks of expectations Closed
Copied to Bug #3597: ftp: asan detects leaks of expectations Closed

History

#1 - 12/04/2019 07:32 PM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Jeff Lucovsky
- Priority changed from Normal to High
- Target version set to 5.0.1

#2 - 12/04/2019 07:42 PM - Jeff Lucovsky
Peter .. Can you apply the diff from 3118 and rerun to see if that's the culprit?

#3 - 12/05/2019 07:07 AM - Peter Manev
Yep - did that now chasing it. Will report back - hopefully today.

#4 - 12/07/2019 03:12 PM - Jeff Lucovsky
- Related to Bug #2458: memleak: gitmaster - 4.1.0-dev (rev c60dec0) added

#5 - 12/13/2019 10:04 AM - Victor Julien
- Target version changed from 5.0.1 to 5.0.2

#6 - 02/13/2020 10:30 AM - Victor Julien
- Target version changed from 5.0.2 to 5.0.3

#7 - 04/03/2020 11:37 AM - Victor Julien
- Subject changed from ftp asan leak to ftp: asan detects leaks of expectations
- Status changed from Assigned to Closed
- Assignee changed from Jeff Lucovsky to Eric Leblond
- Priority changed from High to Normal
- Target version changed from 5.0.3 to 6.0.0rc1
- Label Needs backport to 4.1, Needs backport to 5.0 added

https://github.com/OISF/suricata/pull/4761

#8 - 04/04/2020 07:02 AM - Victor Julien
- Has duplicate Bug #3455: asan ftp related leaks on the current gitmaster added

#9 - 04/04/2020 08:25 AM - Peter Manev
Still see that with - Suricata version 6.0.0-dev (09a21545c 2020-04-03)

```
```

```
==99654==ERROR: LeakSanitizer: detected memory leaks
Direct leak of 29088 byte(s) in 909 object(s) allocated from:
  #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
  #1 0x7f61f3ba342e in jansson_alloc (/lib/x86_64-linux-gnu/libjansson.so.4+0x842e)
Direct leak of 180 byte(s) in 18 object(s) allocated from:
  #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
  #1 0x7f61f3910d84 in pcre_get_substring (/lib/x86_64-linux-gnu/libpcre.so.3+0x28d84)
Direct leak of 32 byte(s) in 1 object(s) allocated from:
  #0 0x4cf63a in calloc (/usr/bin/suricata+0x4cf63a)
```

05/27/2020
Indirect leak of 3105 byte(s) in 207 object(s) allocated from:
  #0 0x4cf4f43 in __interceptor_malloc (/usr/bin/suricata+0x4cf4f43)
  #1 0x7f61f3ba0b14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
  #2 0x32332e383730 (<unknown module>)

Indirect leak of 1666 byte(s) in 119 object(s) allocated from:
  #0 0x4cf4f43 in __interceptor_malloc (/usr/bin/suricata+0x4cf4f43)
  #1 0x7f61f3ba0b14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
  #2 0x3430312e2f (<unknown module>)

Indirect leak of 1176 byte(s) in 84 object(s) allocated from:
  #0 0x4cf4f43 in __interceptor_malloc (/usr/bin/suricata+0x4cf4f43)
  #1 0x7f61f3ba0b14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)

#10 - 04/04/2020 10:45 AM - Victor Julien
  - Status changed from Closed to Assigned

Ok, so not fixed. Btw there are more leaks in there around eve.json.

#11 - 04/04/2020 09:29 PM - Peter Manev
  Yes.
  So in a different angle of the chase of this leak. I simply reverted the search and started Suricata with BP filter that negates ftp and ftp-data
  not port ftp or ftp-data

After some runs and back and forts I came up with this leak (it seems non related to the issue here) - wondering if it is connected somehow or it needs its separate issue.

```c
```

=================================================================
==9040==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 53728 byte(s) in 1679 object(s) allocated from:
  #0 0x4cf4f43 in __interceptor_malloc (/usr/bin/suricata+0x4cf4f43)
  #1 0x7f9cc32b142e (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x842e)

Direct leak of 180 byte(s) in 18 object(s) allocated from:
  #0 0x4cf4f43 in __interceptor_malloc (/usr/bin/suricata+0x4cf4f43)
  #1 0x7f9cc301ed84 in pcre_get_substring (/lib/x86_64-linux-gnu/libpcre.so.3+0x28d84)

Direct leak of 116 byte(s) in 1 object(s) allocated from:
  #0 0x4cf8f62 in realloc (/usr/bin/suricata+0x4cf8f62)
```
```
Indirect leak of 16081 byte(s) in 1237 object(s) allocated from:

0x4cf443 in __interceptor_mallo...
Indirect leak of 658 byte(s) in 47 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x38332e3933 (unknown module)

Indirect leak of 546 byte(s) in 39 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x39322e3933 (unknown module)

Indirect leak of 285 byte(s) in 19 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x3839312e3030 (unknown module)

Indirect leak of 252 byte(s) in 21 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x352e2f (unknown module)

Indirect leak of 238 byte(s) in 17 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x3737312e2f (unknown module)

Indirect leak of 182 byte(s) in 13 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x3330312e2f (unknown module)

Indirect leak of 150 byte(s) in 10 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x33332e3933 (unknown module)

Indirect leak of 126 byte(s) in 9 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x33332e3933 (unknown module)

Indirect leak of 84 byte(s) in 7 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x33332e3933 (unknown module)

Indirect leak of 70 byte(s) in 5 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x33332e3933 (unknown module)

Indirect leak of 48 byte(s) in 3 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x33332e3933 (unknown module)

Indirect leak of 30 byte(s) in 2 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x33332e3933 (unknown module)

Indirect leak of 20 byte(s) in 2 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x660030 in ModbusParseWriteRequest /opt/suricata/src/app-layer-modbus.c:789:33

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
- #1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
- #2 0x3334312e343231 (unknown module)

Indirect leak of 13 byte(s) in 1 object(s) allocated from:
- #0 0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
Indirect leak of 12 byte(s) in 1 object(s) allocated from:
0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
#1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
#2 0x3333312d (<unknown module>)

Indirect leak of 12 byte(s) in 1 object(s) allocated from:
0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
#1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
#2 0x30322d (<unknown module>)

Indirect leak of 11 byte(s) in 1 object(s) allocated from:
0x4cf443 in __interceptor_malloc (/usr/bin/suricata+0x4cf443)
#1 0x7f9cc32aeb14 (/usr/lib/x86_64-linux-gnu/libjansson.so.4+0x5b14)
#2 0x352d (<unknown module>)

SUMMARY: AddressSanitizer: 76340 byte(s) leaked in 3377 allocation(s).

#12 - 04/05/2020 09:10 AM - Peter Manev
Opened a separate issue here - [https://redmine.openinfosecfoundation.org/issues/3595](https://redmine.openinfosecfoundation.org/issues/3595) for that last update above ([https://redmine.openinfosecfoundation.org/issues/3378#note-11](https://redmine.openinfosecfoundation.org/issues/3378#note-11)).

#13 - 04/05/2020 01:58 PM - Jeff Lucovsky
- Copied to Bug #3596: ftp: asan detects leaks of expectations added

#14 - 04/05/2020 01:58 PM - Jeff Lucovsky
- Copied to Bug #3597: ftp: asan detects leaks of expectations added

#15 - 05/10/2020 01:34 PM - Victor Julien
- Status changed from Assigned to Closed

Despite trying hard none of us have been able to reproduce this either in targeted testing or in our general sensors. So considering fixed.