Suricata - Support #3415

Suricata 5.0.1 broken (undefined symbol: htp_connp_req_close)
12/14/2019 08:14 AM - Roman Gugelhupf

Status: Closed
Priority: Normal
Assignee: 
Category: 
Affected Versions: 5.0.1
Label: 

Description

Suricata 5.0.1 seems to be broken, throwing the following error message:

suricata: symbol lookup error: suricata: undefined symbol: htp_connp_req_close

Installation:

```
git clone https://github.com/OISF/suricata.git
cd suricata
git clone https://github.com/OISF/libhtp
cd libhtp
sh autogen.sh
cd ..
./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var --enable-luajit --enable-geoip
make
sudo make install
```

Start Suricata:

```
/usr/bin/suricata -c /etc/suricata/suricata.yaml
```

Suricata does not start:

```
/usr/bin/suricata: symbol lookup error: /usr/bin/suricata: undefined symbol: htp_connp_req_close
```

OS: Ubuntu 18.04.3 LT

History

#1 - 12/14/2019 08:18 AM - Roman Gugelhupf

Not sure, but maybe this problem is related to the latest libhtp commit?

[https://github.com/OISF/libhtp/commit/d806b15c15cf563e5b54c4750a18f61e6ad5a08#diff-1cd979309246d6f03c673987ba0a3e]

Can anyone verify this?

#2 - 12/14/2019 09:55 AM - Victor Julien

What is the output of 'ldd /usr/bin/suricata' ?

#3 - 12/14/2019 09:55 AM - Victor Julien

- Priority changed from Urgent to Normal

#4 - 12/14/2019 11:35 AM - Roman Gugelhupf

```
$ ldd /usr/bin/suricata
linux-vdso.so.1 (0x0000007f76f00000)
libhtp.so.2 => /lib/local/lib/libhtp.so.2 (0x0000007f5dd1f8c000)
libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x0000007f5dd1d8000)
librt.so.1 => /lib/x86_64-linux-gnu/librt.so.1 (0x0000007f5dd1b70000)
libm.so.6 => /lib/x86_64-linux-gnu/libm.so.6 (0x0000007f5dd1822000)
```
liblz4.so.1 => /usr/lib/x86_64-linux-gnu/liblz4.so.1 (0x00007f5dd1606000)
libmaxminddb.so.0 => /usr/lib/x86_64-linux-gnu/libmaxminddb.so.0 (0x00007f5dd1400000)
libluajit-5.1.so.2 => /usr/lib/x86_64-linux-gnu/libluajit-5.1.so.2 (0x00007f5dd187000)
libmagic.so.1 => /lib/x86_64-linux-gnu/libmagic.so.1 (0x00007f5dd0f65000)
libcng.so.0 => /lib/x86_64-linux-gnu/libcng.so.0 (0x00007f5dd0d60000)
libpcap.so.0.8 => /usr/lib/x86_64-linux-gnu/libpcap.so.0.8 (0x00007f5dd0b1f000)
libnet.so.1 => /usr/lib/x86_64-linux-gnu/libnet.so.1 (0x00007f5dd0905000)
libjansson.so.4 => /usr/lib/x86_64-linux-gnu/libjansson.so.4 (0x00007f5dd06f7000)
libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007f5dd04d8000)
libyaml-0.so.2 => /lib/x86_64-linux-gnu/libyaml-0.so.2 (0x00007f5dd02ba000)
libpcre.so.3 => /lib/x86_64-linux-gnu/libpcre.so.3 (0x00007f5dd0048000)
libz.so.1 => /lib/x86_64-linux-gnu/libz.so.1 (0x00007f5dcfe2b000)
libhs.so.4 => /usr/lib/x86_64-linux-gnu/libhs.so.4 (0x00007f5dcf326000)
libnspr4.so => /usr/lib/x86_64-linux-gnu/libnspr4.so (0x00007f5dceda5000)
libnss3.so => /usr/lib/x86_64-linux-gnu/libnss3.so (0x00007f5dcefe2000)
/lib64/ld-linux-x86-64.so.2 (0x00007f5dd2968000)
libstdc++.so.6 => /usr/lib/x86_64-linux-gnu/libstdc++.so.6 (0x00007f5dce413000)
libplc4.so => /usr/lib/x86_64-linux-gnu/libplc4.so (0x00007f5dcdff000)
libplds4.so => /usr/lib/x86_64-linux-gnu/libplds4.so (0x00007f5dcddd6000)

---

### #5 - 12/14/2019 12:13 PM - Victor Julien

libhtp is taken from /usr/local:

```
libhtp.so.2 => /usr/local/lib/libhtp.so.2 (0x00007f5d1fccc000)
```

The new libhtp should have been installed in `/usr/lib` instead. Can you check if there is a more recent libhtp there? I suspect the `/usr/local/lib` version is a leftover from an older install. If you remove that, it should pick up the correct one.

### #6 - 12/14/2019 12:24 PM - Roman Gugelhupf

Thanks Victor. I've removed `/usr/local/lib/libhtp*`, re-compiled it and it seems to work now. However, I'm a bit confused because my understanding was that suricata would take the bundled libhtp version:

```
Non-bundled http: no
```

So, `--enable-non-bundled-htp` would take the libhtp version that is currently installed by the system, while per default suricata uses the one that is bundled. No?

### #7 - 12/14/2019 01:01 PM - Victor Julien

During compilation this is how it works. After Suricata is installed however, it will use the libhtp from your library paths (configured in ld.so.conf). I think in your case `/usr/local/lib` took precedence over `/usr/lib`.

Not sure if we can lock the path at which suri looks for libhtp somehow.

### #8 - 12/14/2019 01:09 PM - Roman Gugelhupf

Ok, thanks Victor for your assistance!

### #9 - 12/14/2019 01:17 PM - Victor Julien

- Tracker changed from Bug to Support
- Status changed from New to Closed

You're welcome!