Suricata - Bug #1715

nfq: broken time stamps with recent Linux kernel 4.4

02/19/2016 11:05 AM - Joachim Schwender

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category: Target version: 3.0.1RC1
Affected Versions: Difficulty:
Effort: Label:

Description

Suricata 3.0 and 2.0.11 have broken time stamps in log files when they run Linux kernel 4.4.0 ... 4.4.2. With older kernels (tested 4.3.3) the time stamp is ok. This blocks the use of suricata on newer kernels.

History

#1 - 02/19/2016 11:21 AM - Peter Manev
I dont seem to be able to reproduce it with 4.4.0 (Debian) and Suricata 3.0 -

```
root@SELKS:~# uname -a
Linux SELKS 4.4.0-stamus-amd64 #1 SMP Sat Feb 6 15:18:09 CET 2016 x86_64 GNU/Linux
```

```
root@SELKS:~# tail -F /var/log/suricata/
certs/ core/ eve-alert.json eve.json fast.log files/
StatsByDate/ stats.log suricata.log suricata-start.log
```

```
root@SELKS:~#
```

```
root@SELKS:~# tail -F /var/log/suricata/fast.log
```

```
```

root@SELKS:~# uname -a
Linux SELKS 4.4.0-stamus-amd64 #1 SMP Sat Feb 6 15:18:09 CET 2016 x86_64 GNU/Linux
```

```
root@SELKS:~# date
Fri Feb 19 12:17:38 EST 2016
```

```
root@SELKS:~# suricata -V
This is Suricata version 3.0 RELEASE
```

Anything specific to your environment ?

#2 - 02/20/2016 04:19 PM - Andreas Herz
- Assignee set to Anonymous
- Target version set to 70

Can you please provide us with used distribution and build-info from suricata?
Couldn't reproduce it either with ArchLinux, Debian, Gentoo and CentOS and 4.4.1 (4.4.2).

#3 - 02/21/2016 12:20 PM - Jay MJ

Andreas Herz wrote:

Can you please provide us with used distribution and build-info from suricata?

I also run ArchLinux x64, latest stable kernel, and could not produce.

#4 - 02/22/2016 12:55 AM - Joachim Schwender

It is production a debian 7.9, with vanilla Kernel 4.3.3 which was ok, and i tested upgrading to kernel 4.4.0 and 4.4.2 which both showed this behaviour. Kernel configuration is the same, and Suricata is currently

This is Suricata version 3.0 RELEASE

and i have observed this also with suricata 2.0.10 and kernel 4.4. glibc is 2.13-1. The hardware is Fujitsu-Siemens R100 with dual Xeon X3430.

#5 - 02/22/2016 02:32 AM - Peter Manev

The bug report cites Debian and there is the same issue reported on the user list about Ubuntu - so something is up I suspect.

As mentioned before - we can not reproduce it on a number of systems (including for Debian 4.4 and 4.4.2 kernel - at least in my tests) - strange.

Anything specific/different the way the kernel/suricata is compiled/installled?

#6 - 02/22/2016 02:35 AM - Victor Julien

Joachim, could you recompile Suricata with the --disable-threading-tls configure flag and see if the issue happens as well?

#7 - 02/22/2016 04:41 AM - Joachim Schwender

i will do that, it will take some time.

#8 - 02/22/2016 04:41 AM - Victor Julien

- Status changed from New to Assigned
- Assignee changed from Anonymous to Victor Julien

#9 - 02/22/2016 07:18 AM - Joachim Schwender

That does not helo. I compiled with --disable-threading-tls booted into kernel 4.4.2 and the log files have broken time stamps. I saw that there were small changes in hrtimer.c in the kernel, but i cannot see why it end up in something like this. Maybe it is a issue with glibc in combination with these kernels.

#10 - 02/25/2016 07:47 AM - Marcel de Groot

I'm also seeing this. Strange thing though:

On two machines (Debian Stretch), both with the same Suricata 3.0 compiled from source with NFQUEUE enabled, and the same kernel, also compiled from source (4.5.0-rc5), one writes the timestamp correctly and the other not:

On the one machine where this symptom plays Suricata is listening via iptables mangle on the FORWARD chain
On the other machine it listens via NFQUEUE in the mangle table on the INPUT and OUTPUT chain. Here the timestamps are correct.

00.000000  

```
02/25/2016-14:32:42.631435  
```

I'll try to check whether changing the NFQUEUE entry makes a difference.

#11 - 02/25/2016 07:49 AM - Victor Julien

Are there differences in time settings? Timezones, etc?

#12 - 02/25/2016 07:56 AM - Marcel de Groot

One addition: I'm seeing this since the 7th of January 2016. Before that the timestamps in fast.log where good. After that the 0 or the 1970... stuff. Not sure what I was running then; I'm guessing kernel 4.4.0 with Suricata 3.0-rc3 or whatever the latest rc of the kernel / Suricata was at the time).

#13 - 02/25/2016 08:19 AM - Joachim Schwender

on my machine i have the following:

```
LANG=de_DE.UTF-8
LC_TIME=en_DK.UTF-8
SHELL=/bin/bash
```

03/14/2022 2/5
iptable uses NFQUEUE as target from INPUT, OUTPUT and FORWARD, not from mangle

#14 - 02/25/2016 03:25 PM - Andreas Herz
Since you all mentioned the use of NFQUEUE i tried that on my machines with 4.4.x kernel and couldn't reproduce it with that mode either. It's seems to be debian/ubuntu specific for now, and even a working debian system from Marcel. Can you provide us with the following infos, so we can gather and compare them:

- suricata --build-info
- exact kernel version and maybe even the config
- other relevant package versions like glibc, libnetfilter_queue especially on the two debian machines that differ somehow
- how you run suricata (commandline)
- system wide time settings

It would be also worth testing other tools that use NFQUEUE to see if they have the same issue on your machines.

#15 - 02/26/2016 03:12 AM - Joachim Schwender
- File sucatat1715.tar.gz added

I am not clear what you mean by system wide time settings?
we run chrony on all machines, and this one is the time reference in our network. setting in /etc/default/locale is LANG="de_DE.UTF-8"

#16 - 02/26/2016 03:14 AM - Joachim Schwender
Suricata log is the only log file with broken time stamps under the conditions mentioned.

#17 - 02/26/2016 04:40 PM - Duarte Silva
Hi lads,
I can reproduce this in a CentOS 7, Kernel is 4.4.2-1.el7.elerepo.x86_64 (from ELRepo) and Suricata is 2.0.11-1.el7.x86_64 (the one compiled by Jason Ish). The timestamps get screwed up.

# date
Fri Feb 26 22:37:18 UTC 2016

# tail -n 1 /var/log/suricata/eve.json
{"timestamp":"1900-01-00T00:00:00.000000","event_type":"dns","src_ip":"8.8.4.4","src_port":53,"dest_ip":"xx.xx.xx.xxx","dest_port":51079,"proto":"UDP","dns":{"type":"answer","id":37092,"rrname":"37092","rrtype":"SOA","ttl":1325}}

This doesn't seem to to happen in the console log though.

# tail /var/log/suricata/suricata.log
26/2/2016 -- 22:17:32 -- <Notice> -- This is Suricata version 2.0.11 RELEASE
26/2/2016 -- 22:17:36 -- <Notice> -- all 1 packet processing threads, 3 management threads initialized, engine started.

Hope it helps,
Duarte

#18 - 02/26/2016 04:51 PM - Andreas Herz
Joachim Schwender wrote:

I am not clear what you mean by system wide time settings?
we run chrony on all machines, and this one is the time reference in our network. setting in /etc/default/locale is LANG="de_DE.UTF-8"

Do you use ntp for example?

@Duarte can you also say how you run suricata (which mode)?

#19 - 02/27/2016 05:57 AM - Duarte Silva
Andreas Herz wrote:

Joachim Schwender wrote:

I am not clear what you mean by system wide time settings?
we run chrony on all machines, and this one is the time reference in our network. setting in /etc/default/locale is LANG="de_DE.UTF-8"

Do you use ntp for example?
I'm running Suricata in workers mode with NFQUEUE (nftables-0.4-3 and libnetfilter_queue-1.0.2-2).

 Does anyone have this problem w/o running NFQUEUE? For NFQUEUE we have a fix/workaround in the git master:
https://github.com/inliniac/suricata/commit/2b263d55a2d0583a2c02e352bfe49064d44d9b39a

It might be it, because sometimes I get the right timestamp, and others the wrong.

I'm going to test newer versions to see if it changes behaviour.

@Duarte can you also say how you run suricata (which mode)?

#22 - 02/29/2016 05:16 AM - Joachim Schwender

Andreas Herz wrote:

Joachim Schwender wrote:

I am not clear what you mean by system wide time settings?
we run chrony on all machines, and this one is the time reference in our network. setting in /etc/default/locale is LANG="de_DE.UTF-8"  

Do you use ntp for example?

@Duarte can you also say how you run suricata (which mode)?

We don't use ntp, we use chrony instead to adjust the system time.

#23 - 02/29/2016 04:25 PM - Andreas Herz

@Joachim can you test the fix/workaround that Victor linked? On the mailinglist we have the first who said that solved the issue at his system.

#24 - 03/01/2016 01:40 AM - Joachim Schwender

Running suricata 3.0 with vanilla kernel 4.4.2 all timestamps are ok in the logs I have in use (dns, fast, stats, suricata-start, suricata) . --disable-threading-tls does not make a difference, so i removed this compile option.

#25 - 03/01/2016 03:04 AM - Joachim Schwender

I can confirm that it also works with vanilla kernel 4.4.3.
We have a workaround/fix in the tree to handle this: https://github.com/inliniac/suricata/commit/2b263d55a2d0583a2c02e352bfe490fd4f42b39a

https://bugzilla.netfilter.org/show_bug.cgi?id=1066

<table>
<thead>
<tr>
<th>Files</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast</td>
<td>4.69 KB</td>
<td>02/19/2016</td>
<td>Joachim Schwender</td>
</tr>
<tr>
<td>sucata1715.tar.gz</td>
<td>197 KB</td>
<td>02/26/2016</td>
<td>Joachim Schwender</td>
</tr>
</tbody>
</table>