Suricata - Feature #4243
Replacing NSS with OpenSSL

12/30/2020 11:38 AM - Michael Tremer

Status: Rejected
Priority: Normal
Assignee:
Category:
Target version:
Effort:
Difficulty:
Label:

Description
Hello,

I would like to know if there is a change that we can migrate suricata from using NSS to OpenSSL. I tried to research why NSS was chosen, but could not find anything on the old mailing list or on here.

Therefore, I would like to ask if OpenSSL would be a suitable replacement. I personally favour it, because OpenSSL has been massively improved since the last big security incidents and is the default library in most Linux distributions and usually performs better in benchmarks compared to others. It is very portable and runs on many architectures and operating systems, which should not limit anyone from using suricata where they like to.

My biggest pain point is that in IPFire we do not use NSS, and I would like to avoid another crypto library. We already have too many and since this is a sensitive part of the software stack, it would simply be better to already use what we have - and on top might be technologically slightly superior. Many other projects (cURL, Chrome, ...) seem to migrate away from NSS to OpenSSL, too.

So, in short, is it possible to migrate or are there any reasons against that I have missed?

History
#1 - 12/30/2020 01:45 PM - Victor Julien
I think some years ago there was debate about whether the OpenSSL license was compatible with GPL. I haven't looked into that at all lately.

However, it may be a moot point as we're currently working towards using the RustCrypto. For a WIP branch see https://github.com/OISF/suricata/pull/5691

#2 - 12/30/2020 01:55 PM - Michael Tremer
Victor Julien wrote in #note-1:

I think some years ago there was debate about whether the OpenSSL license was compatible with GPL. I haven't looked into that at all lately.

I am not an expert on this, but since loads of GPL-licensed software is using it, I did not consider that a concern.

However, it may be a moot point as we're currently working towards using the RustCrypto. For a WIP branch see https://github.com/OISF/suricata/pull/5691

In that case, I thank you for your answer and will await the works on the Rust port to complete. Do you have a release that you are targeting for this?

#3 - 12/30/2020 02:01 PM - Victor Julien
Yeah this is going into Suricata 7.

#4 - 12/30/2020 02:11 PM - Michael Tremer
Victor Julien wrote in #note-3:

Yeah this is going into Suricata 7.

Thank you. Could you please close this ticket then? I do not seem to have the rights to do that.
Rejecting as we're moving to RustCrypto.