Suricata - Bug #3690

eve.json windows timestamp field has "Eastern Daylight Time" appended to timestamp

05/04/2020 03:25 PM - Bryan Jones

<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>Victor Julien</td>
</tr>
<tr>
<td>Category:</td>
<td>Target version: 6.0.0rc1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>5.0.2</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>Needs backport, Needs backport to 4.1, Needs backport to 5.0</td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description

I am running Suricata-5.0.2-1-64bit.exe suricata install on windows. When I try to import the json data into mysql using this tool, https://github.com/beave/meer, it fails on windows because the timestamp looks like this "2020-05-04T01:08:06.39502Eastern Daylight Time" In linux it looks like this. "2020-05-04T01:08:06.3950273-0400.

Note I am typing these out because the systems are not on this machine and I can't copy paste between them easily. So ignore minor time error details in case I misstyped

Is this something I can adjust in a config file, if not, can you point me to the code where this is handled so that I can strip out the "Eastern Daylight Time" string from the timestamp?

thanks

Related issues:

Copied to Bug #3723: eve.json windows timestamp field has "Eastern Daylight T... New
Copied to Bug #3724: eve.json windows timestamp field has "Eastern Daylight T... New

History

#1 - 05/04/2020 03:31 PM - Bryan Jones
This looks like the relevant commit. https://github.com/OISF/suricata/commit/b12c53cd51ca1b24039c248f1eab6808d9686e4b

Bryan Jones wrote:

I am running Suricata-5.0.2-1-64bit.exe suricata install on windows. When I try to import the json data into mysql using this tool, https://github.com/beave/meer, it fails on windows because the timestamp looks like this "2020-05-04T01:08:06.39502Eastern Daylight Time" In linux it looks like this. "2020-05-04T01:08:06.3950273-0400.

Note I am typing these out because the systems are not on this machine and I can't copy paste between them easily. So ignore minor time error details in case I misstyped

Is this something I can adjust in a config file, if not, can you point me to the code where this is handled so that I can strip out the "Eastern Daylight Time" string from the timestamp?

thanks

#2 - 05/05/2020 12:18 PM - Victor Julien

Some discussion about this here on the MinGW mailinglist: https://sourceforge.net/p/mingw/mailman/message/16286257/
Includes a workaround suggestion.

#3 - 05/12/2020 08:03 PM - Victor Julien
- Tracker changed from Support to Bug
- Status changed from New to Assigned
- Assignee set to Victor Julien
- Target version set to 6.0.0rc1
- Label Needs backport added

#4 - 05/12/2020 08:04 PM - Victor Julien
- Label Needs backport to 4.1, Needs backport to 5.0 added

#5 - 05/25/2020 07:05 AM - Victor Julien
https://github.com/OJSF/suricata/pull/4976/commits/bbdc11842d324005567bac5eafdea5fd0fc62688

#6 - 05/25/2020 07:05 AM - Victor Julien
- Status changed from Assigned to Closed

#7 - 05/25/2020 11:40 AM - Jeff Lucovsky
- Copied to Bug #3723: eve.json windows timestamp field has "Eastern Daylight Time" appended to timestamp added

#8 - 05/25/2020 11:41 AM - Jeff Lucovsky
- Copied to Bug #3724: eve.json windows timestamp field has "Eastern Daylight Time" appended to timestamp added