Suricata - Bug #5388

Bug # 5386 (Closed): detect/threshold: offline time handling issue

detect/threshold: offline time handling issue (5.0.x backports)

06/08/2022 01:26 AM - Juliana Fajardini Reichow

<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>Jeff Lucovsky</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>5.0.10</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>5.0.9</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description

Due to the TIMEVAL_DIFF_SEC calculating the delta into an unsigned integer, it would underflow to a high positive value leading to an incorrect result if the packet timestamp was below the timestamp for the threshold entry.

In normal conditions, this shouldn't happen, but in offline mode, each thread has its own concept of time which might differ significantly based on the pcap. In this case the overflow would be very common.

(Taken from the commit message for the fix, as seen in the WIP PR https://github.com/OISF/suricata/pull/7501)

History

#1 - 06/14/2022 02:26 PM - Jeff Lucovsky
- Subject changed from detect/threshold: offline time handling issue (5.0.x backports to detect/threshold: offline time handling issue (5.0.x backports)
- Status changed from New to In Progress
- Assignee changed from OISF Dev to Jeff Lucovsky

#2 - 06/15/2022 01:18 PM - Jeff Lucovsky
Cherry-pick commit(s)
- df2e408d96d0e37a0599f885dc29ff4011f8899

#3 - 06/15/2022 02:25 PM - Jeff Lucovsky
- Status changed from In Progress to In Review

https://github.com/OISF/suricata/pull/7547

#4 - 06/18/2022 05:21 AM - Victor Julien
- Status changed from In Review to Closed

https://github.com/OISF/suricata/pull/7559/commits/72fad4a9f8be9dbc35a445fca572f8e69e7ec27