Suricata - Feature #933
add a IPv6 (RFC2460 recommended order of EH) rule to decoder events rules

08/29/2013 02:59 AM - Peter Manev

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>low</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>medium</td>
</tr>
</tbody>
</table>

Description
Using Suricata 1.4.5 and beta.

Three pcaps attached -
AbnormalOrderIPv6NonRFC2460Recommended.pcap
AbnormalOrderIPv6HopByHopNotFirst.pcap
AbnormalOrderIPv6HopByHopNotFirst-2.pcap

RFC2460 recommends the order in which they should be chained in an IPv6 packet:
1. IPv6 main header
2. Hop-by-Hop Options header (if present, it MUST be the first one following the main/regular header)
3. Destination Options header
4. Routing header
5. Fragment header
6. Authentication header
7. Encapsulating Security Payload header
8. Destination Options header
9. Upper-layer header
The only MUST requirement is that the Hop-by-Hop EH has to be the first one.

Ref: http://www.ietf.org/rfc/rfc2460.txt

The above mentioned pcaps (attached) mimic the opposite of the recommendations and requirements of the RFC2460

In AbnormalOrderIPv6NonRFC2460Recommended.pcap - the Extension Headers are not ordered as recommended in RFC2460

In AbnormalOrderIPv6HopByHopNotFirst.pcap - the Hop By Hop extension header is present and not first after the main/regular header.
In AbnormalOrderIPv6HopByHopNotFirst-2.pcap - the Hop By Hop extension header is present and not first after the main/regular header.

Currently Suricata does not alert in those cases where the order of EH is against the recommended by RFC2460. It could be helpful to include such a rule.

History
#1 - 09/17/2013 02:40 AM - Victor Julien
  - Assignee set to OISF Dev
  - Target version set to 2.0rc2

#2 - 09/17/2013 02:43 AM - Anoop Saldanha
  - Assignee changed from OISF Dev to Anoop Saldanha

#3 - 11/14/2013 12:03 PM - Victor Julien
  - Status changed from New to Assigned
  - Priority changed from Normal to Low
  - Target version changed from 2.0rc2 to 2.0beta2

03/16/2022
#4 - 12/02/2013 02:57 AM - Victor Julien
- Status changed from Assigned to New
- Assignee changed from Anoop Saldanha to OISF Dev
- Target version changed from 2.0beta2 to 3.0RC2

#5 - 05/20/2015 06:09 AM - Victor Julien
- Target version changed from 3.0RC2 to 70

#6 - 08/09/2018 10:31 AM - Victor Julien
- Assignee changed from OISF Dev to Anonymous
- Priority changed from Low to Normal
- Target version changed from 70 to TBD
- Effort set to low
- Difficulty set to medium

#7 - 02/23/2019 10:13 PM - Andreas Herz
- Assignee set to Community Ticket

Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>AbnormalOrderIPv6HopByHopNotFirst.pcap</td>
<td>110 Bytes</td>
<td>08/29/2013</td>
<td>Peter Manev</td>
</tr>
<tr>
<td>AbnormalOrderIPv6HopByHopNotFirst-2.pcap</td>
<td>110 Bytes</td>
<td>08/29/2013</td>
<td>Peter Manev</td>
</tr>
<tr>
<td>AbnormalOrderIPv6NonRFC2460Recommended.pcap</td>
<td>118 Bytes</td>
<td>08/29/2013</td>
<td>Peter Manev</td>
</tr>
</tbody>
</table>