strongSwan - Bug #3160
No discarding of IKE_SA_INIT messages from responder with cookie with length > 64 octets
27.08.2019 16:01 - Thomas Herlinghaus

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
<th>Start date:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td>Tobias Brunner</td>
<td>Estimated time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Category:</td>
<td>libcharon</td>
<td>Target version:</td>
<td>5.8.1</td>
</tr>
<tr>
<td>Target version:</td>
<td>5.8.1</td>
<td>Affected version:</td>
<td>5.8.0</td>
</tr>
<tr>
<td>Resolution:</td>
<td>Fixed</td>
<td>Assigned by:</td>
<td>Tobias Brunner</td>
</tr>
</tbody>
</table>

Description

A preliminary examination of an acceptance test with an IKE/IPsec test suite (achelos GmbH, Paderborn) unfortunately leads to incorrect test results. Among others there is an error regarding RFC7296 chapter 2.6.

Test scenario: Verify that TOE ignores the COOKIE notification whose length is larger than 64. Here, the length of COOKIE notification is 65.

Result: The TOE responds with the long COOKIE instead of ignoring this one.

Can you confirm this behaviour?
Can you specify the location in the source code that makes the check?

Thanks in advance!

Attached you will find the charon-log and the pcap-file

Associated revisions
Revision 902f38dd - 28.08.2019 12:15 - Tobias Brunner
ikev2: Check the length of received COOKIE notifies

As specified by RFC 7296, section 2.6, the data associated with COOKIE notifications MUST be between 1 and 64 octets in length (inclusive).

Fixes #3160.

History

#1 - 27.08.2019 18:38 - Tobias Brunner
- Tracker changed from Issue to Bug
- Category set to libcharon
- Status changed from New to Feedback
- Target version set to 5.8.1

Can you confirm this behaviour?

Yes.

Can you specify the location in the source code that makes the check?

There is currently no check at all. Not sure why as the original IKEv2 RFC already had that restriction.

I pushed a fix to the 3160-cookie-len branch.

#2 - 28.08.2019 09:06 - Thomas Herlinghaus
I can confirm the fix.

Wed, 2019-08-28 06:55 12[NET] <iketest|1> received packet: from 192.168.221.116 to 192.168.221.129 (115 bytes)
Wed, 2019-08-28 06:55 12[ENC] <iketest|1> invalid notify data length for COOKIE (65)

20.03.2020
Many thanks for the prompt support!

#3 - 28.08.2019 12:19 - Tobias Brunner

- Status changed from Feedback to Closed
- Assignee set to Tobias Brunner
- Resolution set to Fixed

Thanks for testing.

Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC7296_Kp.2.6_2-02.pcap</td>
<td>8.3 KB</td>
<td>27.08.2019</td>
<td>Thomas Herlinghaus</td>
</tr>
<tr>
<td>charon.log</td>
<td>46.7 KB</td>
<td>27.08.2019</td>
<td>Thomas Herlinghaus</td>
</tr>
</tbody>
</table>