strongSwan - Bug #657

strongSwan responds incorrectly to an IKE_SA_INIT request message containing an invalid major version in the IKE header


<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>Martin Willi</td>
</tr>
<tr>
<td>Category:</td>
<td>libcharon</td>
</tr>
<tr>
<td>Target version:</td>
<td>5.2.1</td>
</tr>
<tr>
<td>Affected version</td>
<td>4.6.3</td>
</tr>
<tr>
<td>Resolution:</td>
<td>Fixed</td>
</tr>
</tbody>
</table>

**Description**

I am testing my strongSwan implementation with an IKE_SA_INIT request message. The request message includes an IKE header with an invalid major version (major version set to 5). strongSwan responds to this message with an IKEv1 message with Exchange Type Informational (type value 5). The IKEv1 response is correctly formatted with a Notification (type value 11) payload with a Notify Message Type INVALID_MAJOR_VERSION (type value 5). My problem is that my tester expects an IKEv2 response to the IKE_SA_INIT request message containing the invalid major version. Can you tell me how to configure strongSwan to respond to this message with an appropriate IKEv2 response message?

**Associated revisions**

Revision 75122b90 - 17.07.2014 09:35 - Martin Willi
receiver: Send a single INVALID_MAJOR_VERSION notify for IKE version > 2

We sent both a notify using IKEv1 and IKEv2. This is a little more aggressive than required, RFC 5996 says we "SHOULD send an unauthenticated Notify message of type INVALID_MAJOR_VERSION containing the highest (closest) version number it supports".

Fixes #657.

**History**

#1 - 17.07.2014 09:42 - Martin Willi
- Tracker changed from Issue to Bug
- Category set to libcharon
- Status changed from New to Assigned
- Assignee set to Martin Willi
- Target version set to 5.2.1
- Resolution set to Fixed

Hi Richard,

strongSwan 4.x could not properly negotiate supported version numbers, as it was implemented by two separate daemons. These daemons where unaware of each other, resulting in the behavior you described.

In 5.x, we now handle both IKEv1 and IKEv2 in a single daemon. Depending on your build configuration, strongSwan sends the INVALID_MAJOR_VERSION in the protocol strongSwan speaks. So I recommend to try a newer release, that should fix your issue.

If both IKEv1 and IKEv2 have been enabled, strongSwan (5.x) sent two notifies for both IKEv1 and IKEv2. This seems a little aggressive, and I changed that with the referenced commit to send the notify message with the highest protocol supported.

Regards
Martin

#2 - 02.09.2014 11:07 - Tobias Brunner
- Status changed from Assigned to Closed