BEEM - Android XMPP - Bug #484

Unable to authenticate after upgrade to rc2

03/02/2013 06:43 PM - Anonymous

Status:	Closed	**Start date:**	03/02/2013
Priority:	Normal	**Due date:**	
Assignee:	Frédéric Barthéléry	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	0.1.8		
Affected version:	0.1.8	**Locale:**	

Description

After installing rc2, I am no longer able to successfully connect to my Openfire 3.8.0 server. My server logs report a buffer underflow, which I believe is during the TLS handshake.

I am using a self-signed cert (which I am prompted to accept, and select "Always") and have "Require SSL/TLS" enabled.

This has been working flawlessly on previous versions. The only thing I did was upgrade Beem.

2013.03.02 12:21:42 org.jivesoftware.openfire.nio.ClientConnectionHandler - [/x.x.x.x:46668] Data Read: org.apache.mina.filter.support.SSLHandler@9c4e62f (HeapBuffer[pos=0 lim=22 cap=64: 17 03 01 00 11 4B 10 D4 FD E6 1A CA 3B 52 B4 DF 2C AF F2 C9 57 C5])
2013.03.02 12:21:42 org.jivesoftware.openfire.nio.ClientConnectionHandler - [/x.x.x.x:46668] unwrap()
2013.03.02 12:21:42 org.jivesoftware.openfire.nio.ClientConnectionHandler - [/x.x.x.x:46668] inNetBuffer: java.nio.DirectByteBuffer[pos=0 lim=22 cap=16921]
2013.03.02 12:21:42 org.jivesoftware.openfire.nio.ClientConnectionHandler - [/x.x.x.x:46668] appBuffer: java.nio.DirectByteBuffer[pos=0 lim=33842 cap=33842]
2013.03.02 12:21:42 org.jivesoftware.openfire.nio.ClientConnectionHandler - [/x.x.x.x:46668] Unwrap res:Status = OK HandshakeStatus = NOT_HANDSHAKING
bytesConsumed = 22 bytesProduced = 1
2013.03.02 12:21:42 org.jivesoftware.openfire.nio.ClientConnectionHandler - [/x.x.x.x:46668] inNetBuffer: java.nio.DirectByteBuffer[pos=22 lim=22 cap=16921]
2013.03.02 12:21:42 org.jivesoftware.openfire.nio.ClientConnectionHandler - [/x.x.x.x:46668] appBuffer: java.nio.DirectByteBuffer[pos=1 lim=33842 cap=33842]
2013.03.02 12:21:42 org.jivesoftware.openfire.nio.ClientConnectionHandler - [/x.x.x.x:46668] Unwrap res:Status = BUFFER_UNDERFLOW HandshakeStatus = NOT_HANDSHAKING
bytesConsumed = 0 bytesProduced = 0
2013.03.02 12:21:42 org.jivesoftware.openfire.nio.ClientConnectionHandler - [/x.x.x.x:46668] appBuffer: java.nio.DirectByteBuffer[pos=0 lim=1 cap=33842]
2013.03.02 12:21:42 org.jivesoftware.openfire.nio.ClientConnectionHandler - [/x.x.x.x:46668] app data read: HeapBuffer[pos=0 lim=1 cap=1: 20] (20)

Device: Galaxy Nexus
Version: 4.2.2
Rooted: no

Thanks for looking at this - I use Beem every day!

What steps will reproduce the problem?
1.
2.
3.

What is the expected output? What do you see instead?

What version of Beem are you using? On what Android version? On what device?

Please provide any additional information below.

What steps will reproduce the problem?
1.
2.
3.

What is the expected output? What do you see instead?

What version of Beem are you using? On what Android version? On what device?

Please provide any additional information below.

Associated revisions

Revision 1027:8198b5e53cac - 03/06/2013 09:30 PM - Frédéric Barthéléry

Scram-Sha-1 mechanism : do not send authzid if it not absolutely necessary

Some servers (ejabberd) reject the challenge if the
scram attributes a (authzid) and n (authcid) are equals
or they just don't handle the authzid.
So we just don't send it if they are the same
This fix #484

History

#1 - 03/02/2013 07:06 PM - John S

Registered to track.

#2 - 03/02/2013 11:56 PM - Frédéric Barthéléry

Can we have the logcat from Beem ?

#3 - 03/05/2013 08:10 PM - Chris Weiland

i have also this problem
the authentification with a Jabber Account over ccc.de is rejected

#4 - 03/05/2013 08:15 PM - Chris Weiland

when give it a upgrade?

#5 - 03/06/2013 06:10 AM - John S

Frédéric Barthéléry wrote:

> Can we have the logcat from Beem ?

It appears both logcat and catlog require my phone to be rooted (it's not). That may take me a couple of days.

In the meantime, I've created an account for you on my server and sent you the details in IM if you'd like to try it yourself.

#6 - 03/06/2013 06:16 AM - John S

I forgot to add, I upgraded my Openfire server to the (now current) version 3.8.1 just to see if it would resolve this issue, but it did not. My other xmpp clients still continue to work as expected.

#7 - 03/06/2013 03:51 PM - Frédéric Barthéléry

- Subject changed from Unable to authenticate after upgrade to rc2 to Unable to authenticate after upgrade to rc2

- Description updated

- Status changed from New to Assigned

- Assignee set to Frédéric Barthéléry

This seems to be a serverside problem (at least for jabber.ccc.de)
The server announced that it supports a more secure authentication mechanism (SCRAM-SHA-1) and Beem try to use it to authenticate (The support for this mechanism was added in 0.1.8). But the server rejects the authentication immediately.
Your other clients use the DIGEST-MD5 mechanism which is less secured.

Here are some logs of the problematic xmpp exchange :

```
D/SMACK   (24061): 03:27:23 PM SENT (1116882216): <stream:stream to="jabber.ccc.de" xmlns="jabber:client" xmln
s:stream="http://etherx.jabber.org/streams" version="1.0">
D/SMACK   (24061): 03:27:23 PM RCV  (1116882216): <?xml version='1.0'?><stream:stream xmlns='jabber:client' xm
lns:stream='http://etherx.jabber.org/streams' id='2855799452' from='jabber.ccc.de' version='1.0' xml:lang='en'
>
```

```
D/SMACK   (24061): 03:27:23 PM RCV  (1116882216): <stream:features><mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'><mechanism>PLAIN</mechanism><mechanism>DIGEST-MD5</mechanism><mechanism>SCRAM-SHA-1</mechanism></mechanisms><c xmlns='http://jabber.org/protocol/caps' hash='sha-1' node='http://www.process-one.net/en/ejabberd/' ver='o8zQAtrb2wELMmZizvbnpvqp5cE='/><register xmlns='http://jabber.org/features/iq-register'/></stream:features>
D/SMACK   (24061): 03:27:23 PM SENT (1116882216): <auth mechanism="SCRAM-SHA-1" xmlns="urn:ietf:params:xml:ns:xmpp-sasl">bixhPWJlZW0sbj1iZWVtLHI9NDA1NzViYjFiODNlYzdlMGFmMjU4ZGFmOGIyNzEwNTQ2OTEzOTFhN2NhZWJjODZmZmU1YWFhMGNhYWMzZWRmMw==</auth>
D/SMACK   (24061): 03:27:23 PM RCV  (1116882216): <failure xmlns='urn:ietf:params:xml:ns:xmpp-sasl'><bad-protocol/></failure>
E/XMPPConnectionAdapter(24061): Error while connecting
E/XMPPConnectionAdapter(24061): SASL authentication failed using mechanism SCRAM-SHA-1:
E/XMPPConnectionAdapter(24061):     at org.jivesoftware.smack.SASLAuthentication.authenticate(SASLAuthentication.java:259)
E/XMPPConnectionAdapter(24061):     at org.jivesoftware.smack.XMPPConnection.login(XMPPConnection.java:207)
E/XMPPConnectionAdapter(24061):     at com.beem.project.beem.service.XmppConnectionAdapter.login(XmppConnectionAdapter.java:251)
E/XMPPConnectionAdapter(24061):     at com.beem.project.beem.service.LoginAsyncTask.doInBackground(LoginAsyncTask.java:100)
E/XMPPConnectionAdapter(24061):     at com.beem.project.beem.service.LoginAsyncTask.doInBackground(LoginAsyncTask.java:57)
E/XMPPConnectionAdapter(24061):     at android.os.AsyncTask$2.call(AsyncTask.java:287)
E/XMPPConnectionAdapter(24061):     at java.util.concurrent.FutureTask.run(FutureTask.java:234)
E/XMPPConnectionAdapter(24061):     at android.os.AsyncTask$SerialExecutor$1.run(AsyncTask.java:230)
E/XMPPConnectionAdapter(24061):     at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1080)
E/XMPPConnectionAdapter(24061):     at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:573)
E/XMPPConnectionAdapter(24061):     at java.lang.Thread.run(Thread.java:856)
```

#8 - 03/06/2013 08:20 PM - Chris Weiland

hello Frederic ,

what can i do with this Problem ? Is this Problem corrigible?
Can you solve the problem with SCRAM-SHA-1?

will there be an update?

best regards

Chris

#9 - 03/06/2013 09:44 PM - Frédéric Barthéléry

- Status changed from Assigned to Resolved

- % Done changed from 0 to 100

Applied in changeset 8198b5e53cac.

#10 - 03/06/2013 09:47 PM - Frédéric Barthéléry

I just push a fix for this. You should be able to connect with scram-sha-1 even on the bogus server.
However, this is an issue on the server side, you may want to contact them in order to signal them that bug.

#11 - 03/07/2013 09:37 PM - Chris Weiland

hello Frédéric ,

Request to CCC.de is now sent out. Could you please make a request? As a programmer, you have even more options.

best regards

Chris

#12 - 03/11/2013 06:01 PM - Chris Weiland

Hello Frédéric ,

when there will be a new update ?

I want to use their software with my account on Android ;-)

#13 - 03/11/2013 06:02 PM - Chris Weiland

PS: i have no feedback from ccc.de ..... more as bad :-(

#14 - 03/12/2013 08:44 AM - Frédéric Barthéléry

Chris Weiland wrote:

> Hello Frédéric ,
>
> when there will be a new update ?
>
> I want to use their software with my account on Android ;-)

There will be an update at the end of the week.

#15 - 03/14/2013 10:17 AM - Frédéric Barthéléry

- Subject changed from Unable to authenticate after upgrade to rc2 to Unable to authenticate after upgrade to rc2

- Description updated

- Status changed from Resolved to Closed

- Target version set to 0.1.8

#16 - 03/14/2013 07:08 PM - Chris Weiland

hello Frédéric ,

many thank you for the today Upgrade **G**

it work with my ccc.de Account and is work so far ...very very good.
I hope the App is not so a Akku Killer as the Jabiru App ;-)

many many thanks for this **G**

PS: have the Conection now with scram-sha-1 or have the conection changed ?

best regards
Chris

#17 - 03/15/2013 10:08 AM - Frédéric Barthéléry

Chris Weiland wrote:

> PS: have the Conection now with scram-sha-1 or have the conection changed ?

It works with scram-sha-1