Item 266
git_comments:

1. 100MB

git_commits:

1. **summary:** https://issues.apache.org/jira/browse/AMQ-498 - prevent dos attack for nio transport by specifying large frame size
   message: https://issues.apache.org/jira/browse/AMQ-498 - prevent dos attack for nio transport by specifying large frame size git-svn-id: https://svn.apache.org/repos/asf/activemq/trunk@1133003 13f79535-47bb-0310-9956-ffa450edef68

github_issues:

github_issues_comments:

github_pulls:

github_pulls_comments:

github_pulls_reviews:

jira_issues:

1. **summary:** Secure the server from simple DoS attacks
   description: Originating from http://forums.logicblaze.com/posts/list/205.page Simply start the 4.0 server (I used the stock config) in another window telnet to localhost 61616 you will receieve: ActiveMQ^[[? 1;2c type asdfasdf The connection will close by itself. All future TCP connections, either from telnet or from real JMS clients, will hang.
   label: code-design
2. **summary:** Secure the server from simple DoS attacks
   description: Originating from http://forums.logicblaze.com/posts/list/205.page Simply start the 4.0 server (I used the stock config) in another window telnet to localhost 61616 you will receieve: ActiveMQ^[[? 1;2c type asdfasdf The connection will close by itself. All future TCP connections, either from telnet or from real JMS clients, will hang.
3. **summary:** Secure the server from simple DoS attacks
   description: Originating from http://forums.logicblaze.com/posts/list/205.page Simply start the 4.0 server (I used the stock config) in another window telnet to localhost 61616 you will receieve: ActiveMQ^[[? 1;2c type asdfasdf The connection will close by itself. All future TCP connections, either from telnet or from real JMS clients, will hang.
4. **summary:** Secure the server from simple DoS attacks
   description: Originating from http://forums.logicblaze.com/posts/list/205.page Simply start the 4.0 server (I used the stock config) in another window telnet to localhost 61616 you will receieve: ActiveMQ^[[? 1;2c type asdfasdf The connection will close by itself. All future TCP connections, either from telnet or from real JMS clients, will hang.
5. **summary:** Secure the server from simple DoS attacks
   description: Originating from http://forums.logicblaze.com/posts/list/205.page Simply start the 4.0 server (I used the stock config) in another window telnet to localhost 61616 you will receieve: ActiveMQ^[[? 1;2c type asdfasdf The connection will close by itself. All future TCP connections, either from telnet or from real JMS clients, will hang.
6. **summary:** Secure the server from simple DoS attacks
   description: Originating from http://forums.logicblaze.com/posts/list/205.page Simply start the 4.0 server (I used the stock config) in another window telnet to localhost 61616 you will receieve: ActiveMQ^[[? 1;2c type asdfasdf The connection will close by itself. All future TCP connections, either from telnet or from real JMS clients, will hang.
7. **summary:** Secure the server from simple DoS attacks
   description: Originating from http://forums.logicblaze.com/posts/list/205.page Simply start the 4.0 server (I used the stock config) in another window telnet to localhost 61616 you will receieve: ActiveMQ^[[?

1;2c type asdfasdf The connection will close by itself. All future TCP connections, either from telnet or from real JMS clients, will hang.

8. **summary:** Secure the server from simple DoS attacks
   description: Originating from http://forums.logicblaze.com/posts/list/205.page Simply start the 4.0 server (I used the stock config) in another window telnet to localhost 61616 you will receieve: ActiveMQ^[[?1;2c type asdfasdf The connection will close by itself. All future TCP connections, either from telnet or from real JMS clients, will hang.
9. **summary:** Secure the server from simple DoS attacks
   description: Originating from http://forums.logicblaze.com/posts/list/205.page Simply start the 4.0 server (I used the stock config) in another window telnet to localhost 61616 you will receieve: ActiveMQ^[[?1;2c type asdfasdf The connection will close by itself. All future TCP connections, either from telnet or from real JMS clients, will hang.
10. **summary:** Secure the server from simple DoS attacks
    description: Originating from http://forums.logicblaze.com/posts/list/205.page Simply start the 4.0 server (I used the stock config) in another window telnet to localhost 61616 you will receieve: ActiveMQ^[[?1;2c type asdfasdf The connection will close by itself. All future TCP connections, either from telnet or from real JMS clients, will hang.

jira_issues_comments:

1. **body:** Much of this is due to our command packets using variable sized data. The size of the data being transmitted is marshalled first and then the data. The demarshalling code should check against a maximum size for each variable item so that no command packet can blow up the VM due to too much memory usage.
   label: code-design
2. I'm unable to crash the transport by doing this with 5.1.0, Hiram. Is this still a problem in 5.1 or have the commands been changed to handle this correctly?
3. Looks fixed
4. No this has not been fixed. To properly fix this the openwire protocol needs to be updated to do limit checks on the data it serializes.
5. I added maxFrameSize to the OpenWireFormat with default size of 100MB. The size will be checked before message unmarshalling (if size prefix is used) and before reading the content in non-blocking case. This should be suffice to protect the broker from DoS attacks. I can imagine a few more variants that we should protect from, but we can deal with them in separate issues.
6. Oh, and maxFrameSize is negotiable between client and server (the lower value will be used). https://cwiki.apache.org/confluence/display/ACTIVEMQ/Configuring+Wire+Formats
7. Fyi, this change broke us. In the future you should try to make changes that are backwards compatible. If they are not, they should be explicitly mentioned in the release notes. In this case, how many people really need it? It could have been that if the maxFrameSize is not explicitly set, then frame size checking would be disabled - as before. I will say, it is a great feature for those who have publicly exposed brokers. Thanks!
8. with http://svn.apache.org/viewvc?rev=1389817&view=rev in 5.7, the default maxFrameSize is unlimited and there is an explicit limit in the xml config for the transportConnector.