# Grouper Bug GRP-911 and GRP-924 - Unauthorized users can delete attribute assignments



Both the Grouper UI and WS have bugs that allow users to delete attribute assignments if they only have read privileges to them. The WS bug affects v1.6, v2.0, and v2.1 (up to 2.1.4). The UI bug affects v2.0 and v2.1 (up to 2.1.4). The bug has been fixed in each of the branches and will also be included in 2.1.5.

## Reproduce the problem

To reproduce the problem, you need an attribute assignment that's assigned to a group (it could be assigned to other objects as well) and a subject that can read both the attribute definition and group.

```
nonAdminSubjectId = "test.subject.0";
groupName1 = "test:testAttributeAssignDeletePrivilegeIssue:testGroup1";  // use this to test WS issue
groupName2 = "test:testAttributeAssignDeletePrivilegeIssue:testGroup2";  // use this to test UI issue
groupName3 = "test:testAttributeAssignDeletePrivilegeIssue:testGroup3";  // use this to confirm the patch
attributeDefName = "test:testAttributeAssignDeletePrivilegeIssue:attributeDef";
attributeDefNameName = "test:testAttributeAssignDeletePrivilegeIssue:attributeDefName";

grouperSession = GrouperSession.startRootSession();
nonAdminSubject = findSubject(nonAdminSubjectId);

// create groups
group1 = new GroupSave(grouperSession).assignName(groupName1).assignCreateParentStemsIfNotExist(true).save();
group2 = new GroupSave(grouperSession).assignName(groupName2).assignCreateParentStemsIfNotExist(true).save();
group3 = new GroupSave(grouperSession).assignName(groupName3).assignCreateParentStemsIfNotExist(true).save();

// create attribute
attributeDef = new AttributeDefSave(grouperSession).assignName(attributeDefName).assignToGroup(true).
assignAttributeDefType(AttributeDefType.attr).save();
attributeDefName = new AttributeDefNameSave(grouperSession, attributeDef).assignName(attributeDefNameName).
save();

// read privileges
group1.grantPriv(nonAdminSubject, AccessPrivilege.READ);
group2.grantPriv(nonAdminSubject, AccessPrivilege.READ);
group3.grantPriv(nonAdminSubject, AccessPrivilege.READ);
attributeDef.getPrivilegeDelegate().grantPriv(nonAdminSubject, AttributeDefPrivilege.ATTR_READ, false);

// add assignments -- this will print out the attribute assign ids (which will be used later)
group1.getAttributeDelegate().assignAttribute(attributeDefName).getAttributeAssign().getId();
group2.getAttributeDelegate().assignAttribute(attributeDefName).getAttributeAssign().getId();
group3.getAttributeDelegate().assignAttribute(attributeDefName).getAttributeAssign().getId();
```

Make sure to make note of the uuids printed out at the end of the GSH above. You need them later.

Now reproduce the issue using Grouper WS (via the Grouper client). Our test subject shouldn't be allowed to delete the assignment. The attributeAssignUuids value in the example comes from the output of the group1 attribute assignment from above.

```
$ grep grouperClient.webService.login grouper.client.properties
grouperClient.webService.login = test.subject.0
$
$ java -jar grouperClient.jar --operation=assignAttributesWs --attributeAssignType=group --
attributeAssignOperation=remove_attr --attributeAssignUuids=498c0b1edaa948b79225fd5c61f10888
Index: 0: attributeAssignType: group, owner: test:testAttributeAssignDeletePrivilegeIssue:testGroup1,
attributeDefNameName: test:testAttributeAssignDeletePrivilegeIssue:attributeDefName, action: assign, values:
none, enabled: T, id: 498c0b1edaa948b79225fd5c61f10888, changed: T, deleted: T, valuesChanged: F
```

Now reproduce the issue using the Grouper UI.

1. Go to the following page: http://localhost:8090/grouper/grouperUi/appHtml/grouper.html?operation=SimpleAttributeUpdate.assignInit (fix the host and port to match yours).
2. Login as the test subject (e.g. test.subject.0)
3. Select owner type = Group
4. Select "Filter". (If you have a lot of attribute assignments, this won't be the best way to reproduce the problem. Instead give the test subject ADMIN privilege on testGroup2 and filter by owner group as well. The test subject still shouldn't be able to delete the assignment since the test subject doesn't have update on the attributeDef.)
5. Delete the assignment on testGroup2.
6. You get a message that says: You are not allowed to edit the attribute assignment
7. Hit OK and refresh the view by hitting "Filter" again. You'll see that the assignment is gone.

## Patch Grouper WS

You need to edit WsAssignAttributeLogic.java. Note, these instructions are tomcat-specific. Note, anytime you see /PATH_TO_GROUPER_WS_TOMCAT/ substitute that for the path to that tomcat, and anytime you see grouperWsAppName, substitute that for the app name you use for grouper WS, which is generally grouper-ws or grouperWs.

Unzip the grouper-ws.jar file in a location where you can compile a classfile. These instructions are for linux, though could be used in windows if you change the path separators (colon to semicolon)

```
$ mkdir /tmp/grouperWsAttrPatch
$ cd /tmp/grouperWsAttrPatch/
$ mkdir temp
$ unzip /PATH_TO_GROUPER_WS_TOMCAT/webapps/grouperWsAppName/WEB-INF/lib/grouper-ws.jar -d temp
$ mkdir -p edu/internet2/middleware/grouper/ws/rest/attribute
$ cp temp/edu/internet2/middleware/grouper/ws/rest/attribute/WsAssignAttributeLogic.java edu/internet2
/middleware/grouper/ws/rest/attribute/
$ rm -rf temp
$ vi edu/internet2/middleware/grouper/ws/rest/attribute/WsAssignAttributeLogic.java
```

Search for the following: attributeAssign.delete();

Replace this:

```
            case remove_attr:
              attributeAssign.delete();
              wsAssignAttributeResult.setDeleted("T");
              wsAssignAttributeResult.setChanged("T");
              break;
```

With this:

```
            case remove_attr:
              // the delete method doesn't check security so need to do it here...
              attributeAssign.retrieveAttributeAssignable().getAttributeDelegate().
assertCanUpdateAttributeDefName(attributeAssign.getAttributeDefName());
              attributeAssign.delete();
              wsAssignAttributeResult.setDeleted("T");
              wsAssignAttributeResult.setChanged("T");
              break;
```

Compile the patched file, note, if you are using Java previous to 1.6, then you need to list out the jar files, instead of the asterisk. Install, and bounce tomcat

```
$ javac -classpath "/PATH_TO_GROUPER_WS_TOMCAT/webapps/grouperWsAppName/WEB-INF/lib/*" -sourcepath . edu
/internet2/middleware/grouper/ws/rest/attribute/WsAssignAttributeLogic.java
$
$ find . -name WsAssignAttributeLogic*
./edu/internet2/middleware/grouper/ws/rest/attribute/WsAssignAttributeLogic$1.class
./edu/internet2/middleware/grouper/ws/rest/attribute/WsAssignAttributeLogic$2.class
./edu/internet2/middleware/grouper/ws/rest/attribute/WsAssignAttributeLogic$3.class
./edu/internet2/middleware/grouper/ws/rest/attribute/WsAssignAttributeLogic.class
./edu/internet2/middleware/grouper/ws/rest/attribute/WsAssignAttributeLogic.java
$
$ cp -R edu /PATH_TO_GROUPER_WS_TOMAT/webapps/grouperWsAppName/WEB-INF/classes/
$ find /PATH_TO_GROUPER_WS_TOMAT/webapps/grouperWsAppName/WEB-INF/classes/edu -name WsAssignAttributeLogic*
/PATH_TO_GROUPER_WS_TOMAT/webapps/grouperWsAppName/WEB-INF/classes/edu/internet2/middleware/grouper/ws/rest
/attribute/WsAssignAttributeLogic$1.class
/PATH_TO_GROUPER_WS_TOMAT/webapps/grouperWsAppName/WEB-INF/classes/edu/internet2/middleware/grouper/ws/rest
/attribute/WsAssignAttributeLogic$2.class
/PATH_TO_GROUPER_WS_TOMAT/webapps/grouperWsAppName/WEB-INF/classes/edu/internet2/middleware/grouper/ws/rest
/attribute/WsAssignAttributeLogic$3.class
/PATH_TO_GROUPER_WS_TOMAT/webapps/grouperWsAppName/WEB-INF/classes/edu/internet2/middleware/grouper/ws/rest
/attribute/WsAssignAttributeLogic.class
/PATH_TO_GROUPER_WS_TOMAT/webapps/grouperWsAppName/WEB-INF/classes/edu/internet2/middleware/grouper/ws/rest
/attribute/WsAssignAttributeLogic.java
```

Note, if you run on a cluster, you should zip up the files in the patch, and copy them to all servers that need them. Make sure the path is grouperWsAppName/WEB-INF/classes/edu/internet2... Also, you should probably copy the source file and the classfiles in case there are further tweaks.

Bounce tomcat.

Test that the patch worked. Try to delete the assignment on testGroup3; it should fail with a privilege exception. Again, specify the correct attributeAssignUuids based on the output when you assigned the attribute to testGroup3.

```
$ java -jar grouperClient.jar --operation=assignAttributesWs --attributeAssignType=group --
attributeAssignOperation=remove_attr --attributeAssignUuids=2f0b31456efb412f8c96580e610492d1
Error with grouper client, check the logs: Bad response from web service: resultCode: EXCEPTION, clientVersion:
2.1.4, attributeAssignType: group, attributeAssignOperation: remove_attr, attributeAssignValues: null,
attributeAssignValueOperation: null, wsOwnerAttributeAssignLookups: null, wsAttributeAssignLookups: Array size:
1: [0]: WsAttributeAssignLookup[uuid=2f0b31456efb412f8c96580e610492d1]
, wsAttributeDefNameLookups: null, wsOwnerStemLookups: null, wsOwnerGroupLookups: null,
wsOwnerMembershipLookups: null, wsOwnerMembershipAnyLookups: null, wsOwnerAttributeDefLookups: null, actions:
null, includeSubjectDetail: false, actAsSubject: null, subjectAttributeNames: null
, paramNames:
, params: null
, wsOwnerSubjectLookups: null
, attributeDefsToReplace: null
, actionsToReplace: null
, attributeDefTypesToReplace: null, edu.internet2.middleware.grouper.exception.InsufficientPrivilegeException:
Subject Subject id: test.subject.0, sourceId: jdbc cannot update attributeDef test:
testAttributeAssignDeletePrivilegeIssue:attributeDef
        at edu.internet2.middleware.grouper.attr.assign.AttributeAssignGroupDelegate.
assertCanUpdateAttributeDefName(AttributeAssignGroupDelegate.java:129)
        at edu.internet2.middleware.grouper.ws.rest.attribute.WsAssignAttributeLogic.assignAttributesHelper
(WsAssignAttributeLogic.java:433)
        at edu.internet2.middleware.grouper.ws.GrouperServiceLogic.assignAttributes(GrouperServiceLogic.java:
5740)
....
```

## Patch Grouper UI

You need to edit SimpleAttributeUpdate.java. Note, these instructions are tomcat-specific. Note, anytime you see /PATH_TO_GROUPER_UI_TOMCAT/ substitute that for the path to that tomcat, and anytime you see grouperUiAppName, substitute that for the app name you use for grouper UI, which is generally grouper.

Unzip the grouper-ui.jar file in a location where you can compile a classfile. These instructions are for linux, though could be used in windows if you change the path separators (colon to semicolon)

```
$ mkdir /tmp/grouperUiAttrPatch
$ cd /tmp/grouperUiAttrPatch/
$ mkdir temp
$ unzip /PATH_TO_GROUPER_UI_TOMCAT/webapps/grouperUiAppName/WEB-INF/lib/grouper-ui.jar -d temp
$ mkdir -p edu/internet2/middleware/grouper/grouperUi/serviceLogic
$ cp temp/edu/internet2/middleware/grouper/grouperUi/serviceLogic/SimpleAttributeUpdate.java edu/internet2
/middleware/grouper/grouperUi/serviceLogic/
$ rm -rf temp
$ vi edu/internet2/middleware/grouper/grouperUi/serviceLogic/SimpleAttributeUpdate.java
```

Search for the following: attributeAssign.delete();

Replace this:

```
      attributeAssign.delete();

      //now we need to check security
      if (!PrivilegeHelper.canAttrUpdate(grouperSession, attributeAssign.getAttributeDef(), loggedInSubject)) {

        String notAllowed = TagUtils.navResourceString("simpleAttributeAssign.assignEditNotAllowed");
        notAllowed = GrouperUiUtils.escapeHtml(notAllowed, true);
        guiResponseJs.addAction(GuiScreenAction.newAlert(notAllowed));
        return;
      }

      //todo check more security, e.g. where it is assigned
```

With this:

```
      // check security
      try {
        attributeAssign.retrieveAttributeAssignable().getAttributeDelegate().assertCanUpdateAttributeDefName
(attributeAssign.getAttributeDefName());
      } catch (edu.internet2.middleware.grouper.exception.InsufficientPrivilegeException e) {
        String notAllowed = TagUtils.navResourceString("simpleAttributeAssign.assignEditNotAllowed");
        notAllowed = GrouperUiUtils.escapeHtml(notAllowed, true);
        guiResponseJs.addAction(GuiScreenAction.newAlert(notAllowed));
        return;
      }

      attributeAssign.delete();
```

Compile the patched file, note, if you are using Java previous to 1.6, then you need to list out the jar files, instead of the asterisk. Install, and bounce tomcat

```
$ javac -classpath "/PATH_TO_GROUPER_UI_TOMCAT/webapps/grouperUiAppName/WEB-INF/lib/*:/PATH_TO_GROUPER_UI_TOMCAT
/lib/*" -sourcepath . edu/internet2/middleware/grouper/grouperUi/serviceLogic/SimpleAttributeUpdate.java
$
$ find . -name SimpleAttributeUpdate*
./edu/internet2/middleware/grouper/grouperUi/serviceLogic/SimpleAttributeUpdate$1.class
./edu/internet2/middleware/grouper/grouperUi/serviceLogic/SimpleAttributeUpdate.class
./edu/internet2/middleware/grouper/grouperUi/serviceLogic/SimpleAttributeUpdate.java
$
$ cp -R edu /PATH_TO_GROUPER_UI_TOMAT/webapps/grouperUiAppName/WEB-INF/classes/
$ find /PATH_TO_GROUPER_UI_TOMAT/webapps/grouperUiAppName/WEB-INF/classes/edu -name SimpleAttributeUpdate*
/PATH_TO_GROUPER_UI_TOMAT/webapps/grouperUiAppName/WEB-INF/classes/edu/internet2/middleware/grouper/grouperUi
/serviceLogic/SimpleAttributeUpdate$1.class
/PATH_TO_GROUPER_UI_TOMAT/webapps/grouperUiAppName/WEB-INF/classes/edu/internet2/middleware/grouper/grouperUi
/serviceLogic/SimpleAttributeUpdate.class
/PATH_TO_GROUPER_UI_TOMAT/webapps/grouperUiAppName/WEB-INF/classes/edu/internet2/middleware/grouper/grouperUi
/serviceLogic/SimpleAttributeUpdate.java
```

Note, if you run on a cluster, you should zip up the files in the patch, and copy them to all servers that need them. Make sure the path is grouperUiAppName/WEB-INF/classes/edu/internet2... Also, you should probably copy the source file and the classfiles in case there are further tweaks.

Bounce tomcat.

Test that the patch worked. Try to delete the assignment on testGroup3.

1. Go to the following page: http://localhost:8090/grouper/grouperUi/appHtml/grouper.html?operation=SimpleAttributeUpdate.assignInit (fix the host and port to match yours).
2. Login as the test subject (e.g. test.subject.0)
3. Select owner type = Group
4. Select "Filter". (If you have a lot of attribute assignments, this won't be the best way to verify the fix. Instead give the test subject ADMIN privilege on testGroup3 and filter by owner group as well. The test subject still shouldn't be able to delete the assignment since the test subject doesn't have update on the attributeDef.)
5. Delete the assignment on testGroup3.
6. You get a message that says: You are not allowed to edit the attribute assignment
7. Hit OK and refresh the view by hitting "Filter" again. You'll see that the assignment is still there.