GRP 519 - A bug in the Grouper UI allows unauthorized users to view user audit logs by URL manipulation

Wiki Home	**Grouper Release Announcements**	**Grouper Guides**	**Grouper Deployment Guide**	**Community Contributions**	**Internal Developer Resources**

Grouper Security Advisory - 21 December 2010

Patches to the Grouper 1.5.x and 1.6.x UI are available which correct a security issue.
Grouper 1.6.3 and later have the security fix.

Affected Systems
================
All versions of the Grouper 1.5 UI. Also, all versions of the Grouper 1.6 UI prior to 1.6.3.

Grouper UI Security Issue
=========================
Current versions of the Grouper UI are capable of revealing user audit logs to unauthorized users.
The user audit logs contain information that may be sensitive, such as the membership changes of groups.
They also contain other details including the subjects that have performed updates and the servers
where the updates were made from. This bug allows all authenticated users to bypass the current security
checks for user audit logs and view all the logs by URL manipulation.

Recommendations
===============
Sites using Grouper 1.5 and Grouper 1.6 should update the file DoUserAuditReportAction.class in the
grouper.war file. Here are the steps:

1. Download the patch for your version of Grouper:

http://www.internet2.edu/grouper/secadv/20101221/grouper_15_patch.tar
http://www.internet2.edu/grouper/secadv/20101221/grouper_16_patch.tar

2. Untar the patch. If you have deployed the Grouper UI as an expanded WAR, then expand the tar in the
application directory that has the WEB-INF directory and you are done. Otherwise, expand the tar in a
temporary directory and continue to steps (3) and (4) to update and redeploy grouper.war.

If you are running Grouper 1.5: tar xfv grouper_15_patch.tar
If you are running Grouper 1.6: tar xfv grouper_16_patch.tar

3. Update the grouper.war file with the patch: jar ufv grouper.war WEB-INF/classes/edu/internet2/middleware/grouper/ui/actions/DoUserAuditReportAction.*

4. Redeploy grouper.war.

Note: If you are running a build of Grouper 1.5 that you got from the SVN branch GROUPER_1_5_BRANCH after
May 3rd, you should use the 1.6 patch. This would have been an unreleased build after 1.5.3.

Verifying the Patch
===================
To verify that the patch has been applied successfully, browse to the following page: /userAudit.do

For instance: https://hostname/grouper/userAudit.do

If the patch has been applied, you should see an error message on the screen and your grouper_error.log file
should have the following error:

Invalid URL for user audit logs or insufficient privileges.